State of Washington
Department of Enterprise Services
Contracts and Legal Division
Master Contracts & Consulting (MCC)

Contract #00212 with Sentinel Offender Services, LLC for Electronic Monitoring of Offenders

The State of Washington on behalf of the WSCA-NASPO Cooperative Purchasing Organization

Under the Authority of
State of Washington, Chapter 39.26 RCW (formerly Chapter 43.19 RCW)

TABLE OF CONTENTS

1.0 OVERVIEW 5

1.1 CONTRACT SCOPE 5
1.2 CONTRACT SCOPE AND MODIFICATIONS 5
1.3 RECITALS 5
1.4 ESTIMATED USAGE 5
1.5 CONTRACT TERM 6
1.6 PURCHASERS/PARTICIPATING ENTITIES 6

2.0 CONTRACT ADMINISTRATION 7

2.1 MCC CONTRACT ADMINISTRATOR 7
2.2 ADMINISTRATION OF CONTRACT 7
2.3 CONTRACTOR SUPERVISION AND COORDINATION 7
2.4 POST AWARD CONFERENCE 7
2.5 CONTRACT MANAGEMENT 7
2.6 CHANGES 8
2.7 CONTRACT ADMINISTRATION FEE 8
2.8 CONTRACT ADMINISTRATION FEE FOR STATE OF WASHINGTON SALES 8
2.9 WASHINGTON'S STATEWIDE VENDOR PAYMENT REGISTRATION 9
2.10 SALES & SUBCONTRACTOR REPORTS 9
2.11 OTHER MCC REQUIRED REPORT(S) 9
2.12 WASHINGTON'S ELECTRONIC BUSINESS SOLUTION (WEBS) 10

3.0 PRICING 10

3.1 PRICE PROTECTION 10
3.2 NO ADDITIONAL CHARGES 10
3.3 VOLUME/PROMOTIONAL DISCOUNTS 10
3.4 NEW PRODUCTS/SERVICES 10
3.5 PRICE ADJUSTMENTS 10

4.0 CONTRACTOR QUALIFICATIONS AND REQUIREMENTS 11

4.1 ESTABLISHED BUSINESS 11
4.2 USE OF SUBCONTRACTORS 11
4.3 SUBCONTRACTS AND ASSIGNMENT 11
4.4 CONTRACTOR AUTHORITY AND INFRINGEMENT 11
4.5 MATERIALS AND WORKMANSHIP 12
4.6 MERCURY CONTENT AND PREFERENCE 12

5.0 DELIVERY REQUIREMENTS 12

5.1 ORDER FULFILLMENT REQUIREMENTS 12
5.2 EQUIPMENT DEMONSTRATION 12
5.3 SHIPPING AND RISK OF LOSS 12
5.4 DELIVERY 13
5.5 SITE SECURITY 13
5.6 INSPECTION AND REJECTION 13
5.7 TREATMENT OF ASSETS 13
5.8 LABELING 14

6.0 PAYMENT 14

6.1 ADVANCE PAYMENT PROHIBITED 14
6.2 IDENTIFICATION 14
6.3 PAYMENT, INVOICING AND DISCOUNTS 14
6.4 TAXES, FEES AND LICENSES 15
6.5 OVERPAYMENTS TO CONTRACTOR 16
6.6 AUDITS 16

7.0 QUALITY ASSURANCE 16

7.1 RIGHT OF INSPECTION 16

7.2 CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS 17
7.3 PRODUCT WARRANTY 17
7.4 WARRANTIES 17
7.5 DATE WARRANTY 17
7.6 COST OF REMEDY 18
7.8 TRAINING 18

8.0 INFORMATION AND COMMUNICATIONS 18

8.1 ADVERTISING 18
8.2 RETENTION OF RECORDS 18
8.3 PROPRIETARY OR CONFIDENTIAL INFORMATION 18
8.4 NON-ENDORSEMENT AND PUBLICITY 19
8.5 PROTECTION OF CONFIDENTIAL AND PERSONAL INFORMATION 19

9.0 GENERAL PROVISIONS 20

9.1 GOVERNING LAW/VENUE 20
9.2 SEVERABILITY 20
9.3 SURVIVORSHIP 20
9.4 INDEPENDENT STATUS OF CONTRACTOR 20
9.5 GIFTS AND GRATUITIES 21
9.6 IMMUNITY AND HOLD HARMLESS 21
9.8 NO WAIVER OF SOVEREIGN IMMUNITY 21
9.9 PERSONAL LIABILITY 21
9.10 INSURANCE 22
9.11 INDUSTRIAL INSURANCE COVERAGE 24
9.12 NONDISCRIMINATION 24
9.13 OSHA AND WISHA REQUIREMENTS 24
9.14 ANTITRUST 24
9.15 WAIVER 24
9.16 APPLICABLE STANDARD TERMS AND CONDITIONS 25

10.0 DISPUTES AND REMEDIES 25

10.1 PROBLEM RESOLUTION AND DISPUTES 25
10.2 ADMINISTRATIVE SUSPENSION 25
10.3 FORCE MAJEURE 26
10.4 ALTERNATIVE DISPUTE RESOLUTION FEES AND COSTS 26
10.5 NON-EXCLUSIVE REMEDIES 26
10.6 LIMITATION OF LIABILITY 26
10.7 FEDERAL FUNDING 27
10.8 FEDERAL RESTRICTIONS ON LOBBYING 27
10.9 FEDERAL DEBARMENT AND SUSPENSION 27

11.0 CONTRACT TERMINATION 27

11.1 MATERIAL BREACH 27
11.2 OPPORTUNITY TO CURE 28
11.3 TERMINATION FOR CAUSE 28
11.4 TERMINATION FOR CONVENIENCE 29
11.5 TERMINATION FOR WITHDRAWAL OF AUTHORITY 29
11.6 TERMINATION FOR NON-ALLOCATION OF FUNDS 29
11.7 TERMINATION FOR CONFLICT OF INTEREST 29
11.8 TERMINATION BY MUTUAL AGREEMENT 30
11.9 TERMINATION PROCEDURE 30

12.0 CONTRACT EXECUTION 31

12.1 PARTIES 31
12.2 ENTIRE AGREEMENT 31
12.3 ORDER OF PRECEDENCE, INCORPORATED DOCUMENTS, CONFLICT AND CONFORMITY 31
12.4 LEGAL NOTICES 32
12.5 LIENS, CLAIMS AND ENCUMBRANCES 33
12.6 AUTHORITY TO BIND 33

12.7 COUNTERPARTS 33

APPENDIX A STANDARD DEFINITIONS 35

APPENDIX B WSCA-NASPO MASTER AGREEMENT STANDARD TERMS AND CONDITIONS 39

APPENDIX C CONTRACTOR INFORMATION AND PROFILE 47

APPENDIX D SPECIFICATIONS 48

APPENDIX E PRICE SHEETS 531

1.0 OVERVIEW

1.1 CONTRACT SCOPE

The purpose of this contract is the purchase of vendor-provided equipment and services for the monitoring of offenders through Radio Frequency (RF) electronic monitoring, alcohol monitoring, transdermal alcohol monitoring, and satellite monitoring and remote tracking service (GPS), (for both one-piece body-attached device and multi-piece device systems). Contracts may be established with one or more vendors for each of these monitoring services and may be modified as necessary to add new technology or enhancements to existing equipment/service available from the contract vendor.

However, during the term of this contract should new methods or types of offender monitoring equipment and/or services become available in the marketplace from a non-contract vendor the state reserves the right to establish separate contracts for such monitoring equipment/services.

1.2 CONTRACT SCOPE AND MODIFICATIONS

The MMC reserves the right to modify this Contract by mutual agreement between the MCC and the Contractor, so long as such modification is substantially within the scope of the original Contract. Such modifications will be evidenced by issuance of a written authorized amendment by the Contract Administrator.

1.3 RECITALS

The state of Washington (acting as the Lead State for the WSCA-NASPO Cooperative Purchasing Organization, referred to as WSCA-NASPO), acting by and through MCC, issued a Request for Proposal for the purpose of purchasing equipment and services for the electronic monitoring of offenders in accordance with its authority under Chapter 39.26 RCW.

Sentinel Offender Services, LLC submitted a timely Response to the MCC's Solicitation (incorporated by reference).

The MCC evaluated all properly submitted Responses to the above-referenced RFP and has identified Sentinel Offender Services, LLC as one of the apparently successful Contractors.

The MCC has determined that entering into a Contract with Sentinel Offender Services, LLC for all categories of electronic monitoring services (Radio Frequency (RF), alcohol, transdermal alcohol, and satellite and remote tracking service (GPS) – for both one-piece body-attached device and multi-piece device systems) will meet Purchaser's needs and will be in Purchaser's best interest.

NOW THEREFORE, MCC awards to Sentinel Offender Services, LLC this Contract, the terms and conditions of which shall govern Contractor's furnishing to Purchasers the equipment and services identified herein for the electronic monitoring of offenders. This Contract is not for personal use.

IN CONSIDERATION of the mutual promises as hereinafter set forth, the parties agree as follows:

1.4 ESTIMATED USAGE

Based on past and/or projected future usage, it is estimated that purchases over the initial three (3) year term of the Contract may approximate $10,000,000 for contract products and services. This estimate was provided solely for the purpose of assisting Bidders in preparing their Response. Orders will be placed by Purchasers (Participating Entities) only on an as needed basis.

The State of Washington/WSCA-NASPO Cooperative Purchasing Organization does not represent or guarantee any minimum level of purchase.

1.5 CONTRACT TERM

The initial term of this contract is for approximately three (3) years from May 1, 2013, or the date of last signature whichever is later, through December 31, 2016 with the option to extend for additional term(s) or portions thereof. Extension for each additional term shall be offered at the sole discretion of the MCC and are subject to written mutual agreement. The total contract term, including the initial term and all subsequent extensions, shall not exceed ten (10) years unless an emergency exists and/or special circumstances require a partial term extension. The MCC reserves the right to extend with all or some of the Contractors, solely determined by the MCC.

1.6 PURCHASERS/PARTICIPATING ENTITIES

Participating Entities

Potential Purchasers/Participating Entities include members of the Western States Contracting Alliance (which was replaced by the WSCA-NASPO Cooperative Purchasing Organization). The WSCA-NASPO Cooperative Purchasing Organization (WSCA-NASPO) is a cooperative group-contracting consortium for state government departments, institutions, institutions of higher education, agencies and political subdivisions (e.g., school districts, counties, cities, etc.,). WSCA-NASPO Cooperative Purchasing Organization is a cooperative purchasing arm of the National Association of State Procurement Officials (NASPO). The balance of the 50 states, the District of Columbia, US Territories and other public entities may also use WSCA-NASPO contracts.

In addition to the State of Washington, the following Participating Entities have signified their intent to participate in this contract: State of Montana, State of Utah, State of South Dakota, State of Hawaii, State of New Mexico, State of Arkansas, State of Virginia, State of Alaska, State of Connecticut, State of Oklahoma, State of California, State of Nevada, State of South Carolina, State of North Dakota, State of Louisiana, State of Michigan, State of Mississippi, and State of Rhode Island. An estimated average number of units in daily usage or an estimated anticipated annual spend amount was provided in the Request for Proposal document to assist vendors in preparing their proposals. Individual state terms and conditions for the states of Utah, Oklahoma, and North Dakota are incorporated by reference into this Contract as was provided in the Request for Proposal document in Appendix H Intent to Participate for Electronic Monitoring of Offenders Contract.

However, this Intent to Participate document is not binding. During the term of this Contract, other states and public entities may use this contract by executing a Participating Addendum between themselves and the Contractor.

Washington State Purchasing Cooperative (WSPC)

Additionally, this Contract may be used by members of the Washington State Purchasing Cooperative (WSPC) including where applicable: State Agencies, Institutions of Higher Education, Political Subdivisions, and Non-Profit Corporations. A list of WSPC members is available at http://www.ga.wa.gov/PCA/SPC.htm

The State of Washington reserves the right to define the delivery process for any and all awarded vendor services for the purpose of sales within Washington State. This includes the right to establish an independent broker to work with prisons, other correctional institutions and other offender monitoring activities.

2.0 CONTRACT ADMINISTRATION

2.1 MCC CONTRACT ADMINISTRATOR

The MCC shall appoint a single point of contact that will be the Contract Administrator for this Contract and will provide oversight of the activities conducted hereunder. The Contract Administrator will be the principal contact for Contractor concerning business activities under this Contract. The MCC will notify Contractor, in writing, when there is a new Contract Administrator assigned to this Contract.

2.2 ADMINISTRATION OF CONTRACT

MCC will maintain Contract information and pricing and make it available on the DES web site.

2.3 CONTRACTOR SUPERVISION AND COORDINATION

Contractor shall:

1. Competently and efficiently, supervise and coordinate the implementation and completion of all Contract requirements specified herein;
2. Identify the Contractor's Representative, who will be the principal point of contact for the MCC Contract Administrator concerning Contractor's performance under this Contract.
3. Immediately notify the Contract Administrator in writing of any change of the designated Contractor's Representative assigned to this Contract; and
4. Violation of any provision of this paragraph may be considered a material breach establishing grounds for Contract termination.
5. Be bound by all written communications given to or received from the Contractor's Representative.

2.4 POST AWARD CONFERENCE

The Contractor may be required to attend a post award conference scheduled by the Procurement Coordinator to discuss contract performance requirements. The time and place of this conference will be scheduled following contract award.

2.5 CONTRACT MANAGEMENT

Upon award of this Contract, the Contractor shall:

1. Review the impact of the award and take the necessary steps needed to ensure that contractual obligations will be fulfilled.
2. Promote and market the use of this Contract to all authorized contract Purchasers/Participating Entities.
3. Ensure that those who endeavor to utilize this Contract are authorized Purchasers/Participating Entities under the terms and conditions of this Contract.
4. At no additional charge, assist Purchasers/Participating Entities in the following manner to make the most cost effective, value based, purchases including, but not limited to:
    a) Visiting the Purchaser/Participating Entities site and providing them with materials/supplies/equipment recommendations.
    b) Providing Purchasers/Participating Entities with a detailed list of contract products and services including current contract pricing.

5. The Contractor shall designate a customer service representative who will be responsible for addressing Purchaser/Participating Entities issues including, but not limited to:
    a) Logging requests for service, ensuring equipment repairs are completed in a timely manner, dispatching service technicians, and processing warranty claim documentation.
    b) Providing Purchasers/Participating Entities with regular and timely status updates in the event of an order or repair fulfillment delay.
6. Acting as the lead and liaison between the Contractor and Purchaser/Participating Entities in resolving warranty claims for Contract items purchased.

2.6 CHANGES

Alterations to any of the terms, conditions, or requirements of this Contract shall only be effective upon written issuance of a mutually agreed Contract Amendment by the Contract Administrator. However, changes to point of contact information may be updated without the issuance of a mutually agreed Contract Amendment.

2.7 CONTRACT ADMINISTRATION FEE

The Contract(s) will be subject to a WSCA-NASPO Administration Fee. Bidder(s) will include this fee in its bid pricing and not as a separate line item to Purchasers/Participating Entities. The Contractor(s) will collect the fees and distribute the fees to WSCA-NASPO as outlined below.

The WSCA-NASPO Administration Fee will be one-half of one percent (0.5%) on all purchases made under authority of the Contract. Purchases are defined as total invoice price less any applicable sales tax. No taxes will be assessed against this WSCA-NASPO Administration Fee.

The WSCA-NASPO Administrative fee shall be paid within sixty (60) days after the end of the calendar quarter. It is the Contractor's responsibility to calculate and remit the Administrative Fee since WSCA-NASPO does not issue an invoice for this fee. Contractor shall indicate the Contract Number 00212 and include with the remittance, a quarterly sales report by WSCA-NASPO contract participant. The administrative fee shall be paid to:

WSCA-NASPO COOPERATIVE PURCHASING ORGANIZATION
PROGRAM MANAGER
201 EAST MAIN STREET, SUITE 1450
LEXINGTON, KY 40507

In addition to the WSCA-NASPO Administration Fee as stated above, some Participating Entities may also require an administrative fee, and it will be incorporated into the Participating Entity's Participating Addendum. Participating Entity Administrative Fees may or may not be added to the price of contract products/services as determined between themselves.

2.8 CONTRACT ADMINISTRATION FEE FOR STATE OF WASHINGTON SALES

Contractor shall pay the Department of Enterprise Services (DES) a fee ("Washington Management Fee") equal to 0.74% of the total invoice price, less any taxes, returns, credits, or adjustments, of all sales ("Total Net Sales") made to Purchasers/Participating Entities located within the state of Washington under this Contract. Contractor shall hold the Management Fee in trust for DES until such fees are remitted to DES.

The Washington Management Fee will be included in Contractor's pricing, as set forth in the Contract (including all amendments), and will not be included as a separate line item on any invoice submitted to a Washington Purchasers/Participating Entities.

DES may, at its sole discretion, increase, decrease, or eliminate the Washington Management Fee upon thirty (30) days written notice to Contractor. Any decrease to or elimination of the Washington Management Fee, shall be reflected in Contract pricing commensurate with the adjustment. DES reserves the right to negotiate Contract pricing with the Contractor when the Washington Management Fee adjustment results in an increase to Contract prices.

Contractor will provide DES with a Sales Report detailing Total Net Sales for the preceding quarter in accordance with the Sales & Subcontractor Reports section of the Contract. DES will send an invoice each quarter, based on the Sales Report within thirty (30) days after receiving the Sales Report. Payment of the Washington Management Fee is due within thirty (30) days of Contractor's receipt of such invoice from DES.

MCC reserves the right to audit, or have a designated third party audit, applicable records to ensure that the state has been properly invoiced and all Washington Management Fees have been paid. Failure to accurately report Total Net Sales, to submit a timely Sales Report, or remit timely payment of the Washington Management Fee, may be cause for Contract termination, the charging of interest or penalties, or the exercise of other remedies provided by law.

Washington Management Fee payment must reference the Contract number and the quarter/year for which the Washington Management Fee is being remitted. All payments must be sent to:

State of Washington
Department of Enterprise Services
Finance Department
Post Office Box 41411
Olympia, WA 98504-1411

2.9 WASHINGTON'S STATEWIDE VENDOR PAYMENT REGISTRATION

Contractors are required to be registered in the Statewide Vendor Payment system, prior to submitting a request for payment from Purchasers located within the state of Washington under this Contract. Purchasers who are Washington state agencies require registration to be completed prior to payment.

The Washington State Office of Financial Management (OFM) maintains a central contractor registration file for Washington State agencies to process contractor payments.

To obtain registration materials go to http://www.ofm.wa.gov/accounting/vendors.asp the form has two parts; Part 1 is the information required to meet the above registration condition. Part 2 allows the state to pay invoices electronically with direct deposit and is the state's most efficient method of payment and you are encouraged to sign up for this form of payment.

2.10 SALES & SUBCONTRACTOR REPORTS

The Contractor shall provide a Sales and Subcontractor Report to the Master Contracts & Consulting on a quarterly basis in the electronic format provided by the Master Contracts & Consulting at: https://fortress.wa.gov/ga/apps/CSR/Login.aspx.

Reports must be submitted electronically within thirty (30) days after the end of the calendar quarter, i.e., no later than April 30th, July 31st, October 31st and January 31st.

2.11 OTHER MCC REQUIRED REPORT(S)

All MMC required reports under this contract must be delivered to the Contract Administrator. Contractor may be required to provide a detailed annual contract sales history report that may include but is not limited to product/service description, per unit quantities/services supplied,

contract price in an electronic format that can be read by MS Excel. Other required reports will be designed and approved by the parties by mutual agreement.

2.12 WASHINGTON'S ELECTRONIC BUSINESS SOLUTION (WEBS)

Contractor shall be registered in the Contractor registration system, Washington's Electronic Business Solution (WEBS) www.ga.wa.gov/webs, maintained by the Washington State Department of Enterprise Services. Contractors already registered need not re-register. It is the sole responsibility of Contractor to properly register with WEBS and maintain an accurate Contractor profile in WEBS.

3.0 PRICING

3.1 PRICE PROTECTION

Contractor warrants that prices of materials, supplies, services, and/or equipment set forth herein do not exceed those charged by the Contractor to any other customer purchasing the same under similar conditions and in like or similar quantities.

3.2 NO ADDITIONAL CHARGES

Unless otherwise specified herein, no additional charges by the Contractor will be allowed including, but not limited to: handling charges such as packing, wrapping, bags, containers, reels; or the processing fees associated with the use of credit cards. Notwithstanding the foregoing, in the event that market conditions, laws, regulations or other unforeseen factors dictate, at the Contract Administrators sole discretion, additional charges may be allowed.

3.3 VOLUME/PROMOTIONAL DISCOUNTS

Contract prices are the maximum or ceiling price Contractor can charge. The Contractor may also offer volume and/or promotional price discounts to Purchasers/Participating Entities.

3.4 NEW PRODUCTS/SERVICES

A Contractor may propose a revision to its contract offerings to reflect technical product upgrades or other changed products and/or services appropriate to the scope of the Contract. These proposed new products/services with associated pricing may be provided to the MCC Contract Administrator for approval. Contract Administrator has the sole discretion to accept or reject such product/service offerings and pricing. New or changed products/services proposed by Contractor must meet the requirements established in the original solicitation document or subsequent revisions. If approved by MCC, the new products/services will be added to the Contract by written amendment.

3.5 PRICE ADJUSTMENTS

At least one hundred twenty (120) calendar days before the end of the current term of this Contract and subsequent extension periods, Contractor may propose purchase price and support (service) rate increases by written notice to the MCC's Contract Administrator. Price adjustments may be taken into consideration by the MCC's Contract Administrator when determining whether to extend this Contract. Price increases will not be considered without supporting documentation sufficient to justify the requested increase. Contractor shall provide a detailed breakdown of their costs upon request.

Contractors shall not make contract extensions contingent on price adjustments.

Documentation must be based on published indices, such as the Producer Price Index and/or the result of increases at the manufacturer's level, incurred after contract commencement date. The grant

of any price adjustment will be at the sole discretion of the MCC and, if granted, shall not produce a higher profit margin for the Contractor than that established by the original contract pricing. The Contractor shall be notified in writing by the Contract Administrator of any price adjustment granted by the MCC, and such price adjustment shall be set forth in a written amendment to the contract.

4.0 CONTRACTOR QUALIFICATIONS AND REQUIREMENTS

4.1 ESTABLISHED BUSINESS

Prior to commencing performance, or prior to that time if required by the MCC, law or regulation, Contractor must be an established business firm with all required licenses, fees, bonding, facilities, equipment and trained personnel necessary to meet all requirements and perform the work as specified in the Solicitation. Contractor shall maintain compliance with these requirements throughout the life of this contract.

The MCC reserves the right to require receipt of proof of compliance with said requirements within ten (10) calendar days from the date of request, and to terminate this Contract as a material breach for noncompliance with any requirement of this paragraph.

4.2 USE OF SUBCONTRACTORS

In accordance with RFP requirements, Contractor agrees to take complete responsibility for all actions of its Subcontractors.

Prior to performance, Contractor shall identify all subcontractors who will perform services in fulfillment of contract requirements, including their name, the nature of services to be performed, address, telephone, facsimile, email, federal tax identification number (TIN), and anticipated dollar value of each subcontract:

The MCC reserves the right to approve or reject any and all Subcontractors that are identified by the Contractor. Any Subcontractors not listed in the Bidder's Response, who are engaged by the Contractor, must be pre-approved, in writing, by the MCC.

Specific restrictions apply to contracting with current or former state employees pursuant to Chapter 42.52 RCW.

4.3 SUBCONTRACTS AND ASSIGNMENT

Contractor shall not Subcontract, assign, or otherwise transfer its obligations under this Contract without the prior written consent of the Contract Administrator. Contractor shall provide a minimum of thirty (30) calendar days advance notification of intent to Subcontract, assign, or otherwise transfer its obligations under this Contract. Violation of this condition may be considered a material breach establishing grounds for Contract termination. The Contractor shall be responsible to ensure that all requirements of the Contract shall flow down to any and all Subcontractors. In no event shall the existence of a Subcontract operate to release or reduce the liability of Contractor to the state for any breach in the performance of the Contractor's duties.

4.4 CONTRACTOR AUTHORITY AND INFRINGEMENT

Contractor is authorized to sell under this Contract, only those materials, supplies, services and/or equipment as stated herein and allowed for by the provisions of this Contract. Contractor shall not represent to any Purchasers that they have the contract authority to sell any other materials, supplies, services and/or equipment. Further, Contractor may not intentionally infringe on other established Washington State Contracts.

4.5 MATERIALS AND WORKMANSHIP

The Contractor shall be required to furnish all materials, supplies, equipment and/or services necessary to perform Contractual requirements. Materials, supplies and workmanship used in the construction of equipment for this Contract shall conform to all applicable federal, state, and local codes, regulations and requirements for such equipment, specifications contained herein, and the normal uses for which intended. Materials, supplies and equipment shall be manufactured in accordance with the best commercial practices and standards for this type of materials, supplies, and equipment.

4.6 MERCURY CONTENT AND PREFERENCE

Contractor shall provide mercury-free products when available. Should mercury-free products not exist, contractors shall provide products with the lowest mercury content available. Contractor shall disclose products that contain added mercury and provide an explanation that includes the amount or concentration of mercury, and justification as to why added mercury is necessary for the function or performance of the product.

The MCC reserves the right to require receipt of proof of compliance with said requirements within ten (10) calendar days from the date of request, and to terminate this Contract as a material breach for noncompliance with any requirement of this paragraph.

5.0 DELIVERY REQUIREMENTS

5.1 ORDER FULFILLMENT REQUIREMENTS

Authorized Purchasers/Participating Entities may place orders against this Contract either in person, electronically, facsimile or by phone. Once an order is issued, the following shall apply:

1. For purposes of price verification and auditing, upon receipt of a purchase order the Contractor shall send the Purchaser an order confirmation notification that identifies applicable Contract prices to be applied to the order.
2. Upon the request of the Purchaser, the Contractor shall supply Purchaser documentation needed to verify Contract pricing compliance.
3. Product damaged prior to acceptance will either be replaced or repaired in an expedited manner at Contractor's expense. Alternatively, at the Purchaser's option, any possible damage to the product can be noted on the receiving report and the cost deducted from final payment.

The Contractor is responsible to verify delivery conditions/requirements with the Purchaser prior to the delivery.

5.2 EQUIPMENT DEMONSTRATION

During the term of the contract the Contractor may be requested by a Purchaser/Participating Entity to provide an on-site demonstration of the equipment and services available through this contract. Such demonstration(s) shall be provided at no additional cost to the Purchaser/Participating Entity at a mutually agreed upon date and location.

5.3 SHIPPING AND RISK OF LOSS

Contractor shall ship all Products purchased pursuant to this Contract, freight prepaid, FOB Purchaser's specified destination. The method of shipment shall be consistent with the nature of the Products and hazards of transportation. Regardless of FOB point, Contractor agrees to bear all risks

of loss, damage, or destruction of the Products ordered hereunder that occurs prior to delivery, except loss or damage attributable to Purchaser's fault or negligence; and such loss, damage, or destruction shall not release Contractor from any obligation hereunder. After delivery, the risk of loss or damage shall be borne by Purchaser, except loss or damage attributable to Contractor's fault or negligence.

5.4 DELIVERY

Delivery of Products must be made during Purchaser's normal work hours and within time frames mutually agreed in writing between the Purchaser and Contractor at the time of order placement.

Failure to comply with agreed upon delivery times may subject Contractor to damages. The Purchaser may refuse shipment when delivered after normal working hours. The Contractor shall verify specific working hours of individual Purchasers and instruct carrier(s) to deliver accordingly. The acceptance by the Purchaser of late performance, with or without objection or reservation by the Purchaser, shall not waive the right to claim damage for such breach, nor preclude the MCC or Purchaser from pursuing any other remedy provided herein, including termination, nor shall such acceptance of late performance constitute a waiver of the requirements for the timely performance of any obligation remaining to be performed by Contractor.

All deliveries are to be made to the applicable delivery location as indicated in the Order Document. When applicable, the Contractor shall take all necessary actions to safeguard items during inclement weather. In no case shall the Contractor initiate performance prior to receipt of written or verbal authorization from authorized Purchasers. Expenses incurred otherwise shall be borne solely by the Contractor.

5.5 SITE SECURITY

While on Purchaser's/Participating Entity's premises, Contractor, its agents, employees, or Subcontractors shall conform in all respects with physical, fire, or other security regulations.

5.6 INSPECTION AND REJECTION

The Purchaser's/Participating Entity's inspection of all materials, supplies and equipment upon delivery is for the purpose of forming a judgment as to whether such delivered items are what was ordered, were properly delivered and ready for Acceptance. Such inspection shall not be construed as final acceptance, or as acceptance of the materials, supplies or equipment, if the materials, supplies or equipment does not conform to contractual requirements. If there are any apparent defects in the materials, supplies, or equipment at the time of delivery, the Purchaser will promptly notify the Contractor. Without limiting any other rights, the Purchaser may require the Contractor to: (1) repair or replace, at Contractor's expense, any or all of the damaged goods; (2) refund the price of any or all of the damaged goods; or (3) accept the return of any or all of the damaged goods.

5.7 TREATMENT OF ASSETS

1. Title to all property furnished by the Purchaser/Participating Entity shall remain with the Purchaser/Participating Entity, as appropriate. Title to all property furnished by the Contractor, the cost for which the Contractor is entitled to be reimbursed as a direct item of cost under this contract, shall pass to and vest in the Purchaser upon delivery of such property by the Contractor and acceptance by the Purchaser. Title to other property, the cost of which is reimbursable to the Contractor under this Contract, shall pass to and vest in the Purchaser upon (i) issuance for use of such property in the performance of this Contract, or (ii) commencement of use of such property in the performance of this Contract, or (iii) reimbursement of the cost thereof by the Purchaser in whole or in part, whichever first occurs.

Title to monitoring equipment or accessories furnished by the Contractor and leased by the Purchaser does not pass to the Purchaser during the performance of this Contract.

2. Any property of the Purchaser furnished to the Contractor shall, unless otherwise provided herein or approved by the Purchaser, be used only for the performance of this Contract.
3. The Contractor shall be responsible for damages as a result of any loss or damage to property of the Purchaser which results from the negligence of the Contractor or which results from the failure on the part of the Contractor to maintain, administer and protect that property in a reasonable manner and to the extent practicable in all instances.
4. If any Purchaser property is lost, destroyed, or damaged, the Contractor shall immediately notify the Purchaser and shall take all reasonable steps to protect the property from further damage.
5. The Contractor shall surrender to the Purchaser all property of the Purchaser prior to settlement upon completion, termination, or cancellation of this contract.
6. All reference to the Contractor under this clause shall also include Contractor's employees, agents or Subcontractors.

5.8 LABELING

Individual shipping cartons shall be labeled with the name of the ordering agency, order number, contract number, contractor, state stock numbers, and where applicable, date of manufacture, batch number, storage requirements, conditions, and recommended shelf life. Contractors are encouraged to offer product packaging with recycled content.

6.0 PAYMENT

6.1 ADVANCE PAYMENT PROHIBITED

No advance payment shall be made for the Products and Services furnished by Contractor pursuant to this Contract.

Notwithstanding the above, maintenance payments, if any, may be made on a quarterly basis at the beginning of each quarter.

This language shall not prohibit Contractor from collecting advance payments from program participants as part of offender-funded programs, when contracted to do so with a Purchaser/Participating Entity.

6.2 IDENTIFICATION

All invoices, packing lists, packages, instruction manuals, correspondence, shipping notices, shipping containers, and other written materials associated with this Contract shall be identified by the Contract number and the applicable Purchaser's/Participating Entity's order number. Packing lists shall be enclosed with each shipment and clearly identify all contents and any backorders.

6.3 PAYMENT, INVOICING AND DISCOUNTS

Payment is the sole responsibility of, and will be made by, the Purchaser/Participating Entity.

Contractor shall provide a properly completed invoice to Purchaser/Participating Entity. All invoices are to be delivered to the address indicated in the purchase order.

Each invoice shall be identified by the associated WSCA-NASPO Contract Number; the Purchaser's/Participating Entity's contract/purchase order number (as applicable), and shall be in U.S. dollars. Invoices shall be prominently annotated by the Contractor with all applicable prompt

payment and/or volume discount(s) and shipping charges unless otherwise specified in the Solicitation. Hard copy credit memos are to be issued when the state has been overcharged.

Invoices for payment will accurately reflect all discounts due the Purchaser/Participating Entity. Invoices will not be processed for payment, nor will the period of prompt payment discount commence, until receipt of a properly completed invoice denominated in U.S. dollars and until all invoiced items are received and satisfactory performance of Contractor has been accepted by the Purchaser/Participating Entity. If an adjustment in payment is necessary due to damage or dispute, any prompt payment discount period shall commence on the date final approval for payment is authorized.

Under Chapter 39.76 RCW , if Purchaser fails to make timely payment(s), Contractor may invoice for 1% per month on the amount overdue or a minimum of $1.00. Payment will not be considered late if a check or warrant is mailed within the time specified. If no terms are specified, net 30 days will automatically apply. Payment(s) made in accordance with Contract terms shall fully compensate the Contractor for all risk, loss, damages or expense of whatever nature and acceptance of payment shall constitute a waiver of all claims submitted by Contractor. If the Purchaser/Participating Entity fails to make timely payment(s) or issuance of credit memos, the Contractor may impose a 1% per month on the amount overdue.

Payment for materials, supplies and/or equipment received and for services rendered shall be made by Purchaser/Participating Entity and be redeemable in U.S. dollars. Unless otherwise specified, the Purchaser's/Participating Entity's sole responsibility shall be to issue this payment. Any bank or transaction fees or similar costs associated with currency exchange procedures or the use of purchasing/credit cards shall be fully assumed by the Contractor.

6.4 TAXES, FEES AND LICENSES

Taxes:

Where required by statute or regulation, the Contractor shall pay for and maintain in current status all taxes that are necessary for Contract performance. Unless otherwise indicated, the Purchaser agrees to pay State of Washington taxes on all applicable materials, supplies, services and/or equipment purchased. No charge by the Contractor shall be made for federal excise taxes and the Purchaser/Participating Entity agrees to furnish Contractor with an exemption certificate where appropriate.

Collection of Retail Sales and Use Taxes:

In general, Contractors engaged in retail sales activities within the State of Washington are required to collect and remit sales tax to Department of Revenue (DOR). In general, out-of-state Contractors must collect and remit "use tax" to Department of Revenue if the activity carried on by the seller in the State of Washington is significantly associated with Contractor's ability to establish or maintain a market for its products in Washington State. Examples of such activity include where the Contractor either directly or by an agent or other representative:

1. Maintains an in-state office, distribution house, sales house, warehouse, service enterprise, or any other in-state place of business;
2. Maintains an in-state inventory or stock of goods for sale;
3. Regularly solicits orders from Purchasers located within the State of Washington via sales representatives entering the State of Washington;
4. Sends other staff into the State of Washington (e.g. product safety engineers, etc.) to interact with Purchasers in an attempt to establish or maintain market(s); or

5. Other factors identified in WAC 458-20 .

Department of Revenue Registration for Out-of-State Contractors:
Out-of-state Contractors meeting any of the above criteria must register and establish an account with the Department of Revenue. Refer to WAC 458-20-193, and call the Department of Revenue at 800-647-7706 for additional information. When out-of-state Contractors are not required to collect and remit "use tax," Purchasers located in the State of Washington are responsible for paying this tax, if applicable, directly to the Department of Revenue.

Fees/Licenses:
After award of Contract, and prior to commencing performance under the Contract, the Contractor shall pay for and maintain in a current status any licenses, fees, assessments, permit charges, etc., which are necessary for Contract performance. It is the Contractor's sole responsibility to maintain licenses and to monitor and determine any changes or the enactment of any subsequent regulations for said fees, assessments, or charges and to immediately comply with said changes or regulations during the entire term of this Contract.

Customs/Brokerage Fees:
Contractor shall take all necessary actions, including, but not limited to, paying all customs, duties, brokerage, and/or import fees, to ensure that materials, supplies, and/or equipment purchased under the Contract are expedited through customs. Failure to do so may subject Contractor to liquidated damages as identified herein and/or to other remedies available by law or Contract. Neither the MCC nor the Purchaser will incur additional costs related to Contractor's payment of such fees.

Taxes on Invoice:
Contractor shall calculate and enter the appropriate Washington State and local sales tax on all invoices. Tax is to be computed on new items after deduction of any trade-in in accordance with WAC 458-20-247.

6.5 OVERPAYMENTS TO CONTRACTOR

Contractor shall refund to Purchaser/Participating Entity the full amount of any erroneous payment or overpayment under this Contract within thirty (30) days' written notice. If Contractor fails to make timely refund, Purchaser may charge Contractor one percent (1%) per month on the amount due, until paid in full.

6.6 AUDITS

The MCC Contract Administrator and/or the Purchaser/Participating Entity reserves the right to audit, or have a designated third party audit, applicable records to ensure that the Purchaser/Participating Entity has been properly invoiced. Any remedies and penalties allowed by law to recover monies determined owed will be enforced. Repetitive instances of incorrect invoicing may be considered complete cause for contract termination.

7.0 QUALITY ASSURANCE

7.1 RIGHT OF INSPECTION

Contractor shall provide right of access to its facilities to MCC, or any of MCC's officers, or to any other authorized agent or official of the state of Washington or other Participating Entity, or the federal government, at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Contract.

7.2 CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS

Any written commitment by Contractor within the scope of this Contract shall be binding upon Contractor. Failure of Contractor to fulfill such a commitment may constitute breach and shall render Contractor liable for damages under the terms of this Contract. For purposes of this section, a commitment by Contractor includes: (i) Prices, discounts, and options committed to remain in force over a specified period of time; and (ii) any warranty or representation made by Contractor in its Response or contained in any Contractor or manufacturer publications, written materials, schedules, charts, diagrams, tables, descriptions, other written representations, and any other communication medium accompanying or referred to in its Response or used to effect the sale to Purchaser.

7.3 PRODUCT WARRANTY

Warranty(ies): Unless otherwise specified, full parts and labor warranty period shall be for a minimum period of one (1) year after receipt of materials or equipment by the Purchaser. All materials or equipment provided shall be new and unused (or like new with no blemishes or defects), of the latest model or design and of recent manufacture.

In the event of conflict between Contract terms and conditions and Contractor's submitted warranty, the Contract terms and conditions shall prevail; except, to afford the Purchaser/Participating Entity maximum benefits, the MCC may avail itself of the Contractor's warranty if deemed more beneficial to the Purchaser/Participating Entity.

7.4 WARRANTIES

Contractor warrants that all materials, supplies, services and/or equipment provided under this Contract shall be fit for the purpose(s) for which intended, for merchantability, and shall conform to the requirements and specifications herein. Acceptance of any materials, supplies, service and/or equipment, and inspection incidental thereto, by the Purchaser shall not alter or affect the obligations of the Contractor or the rights of the Purchaser.

The Contractor warrants for a period of one year(s) from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the solicitation or for which the Participating Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects. Upon breach of the warranty, the Contractor will repair or replace (at no charge to the Participating Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

7.5 DATE WARRANTY

Contractor warrants that all Products provided under this Contract: (i) do not have a life expectancy limited by date or time format; (ii) will correctly record, store, process, and present calendar dates; (iii) will lose no functionality, data integrity, or performance with respect to any date; and (iv) will be interoperable with other software used by Purchaser that may deliver date records from the Products, or interact with date records of the Products ("Date Warranty"). In the event a Date Warranty problem is reported to Contractor by Purchaser and such problem remains unresolved after three (3) calendar days, at Purchaser's discretion, Contractor shall send, at Contractor's sole

expense, at least one (1) qualified and knowledgeable representative to Purchaser's premises. This representative will continue to address and work to remedy the failure, malfunction, defect, or nonconformity on Purchaser's premises. This Date Warranty shall last perpetually. In the event of a breach of any of these representations and warranties, Contractor shall indemnify and hold harmless Purchaser from and against any and all harm, injury, damages, costs, and expenses incurred by Purchaser arising out of said breach.

7.6 COST OF REMEDY

Cost of Remedying Defects: All defects, indirect and consequential costs of correcting, removing or replacing any or all of the defective materials or equipment will be charged against the Contractor.

7.8 TRAINING

Customer and offender training shall be as specified and described in *Appendix D Specifications*.

8.0 INFORMATION AND COMMUNICATIONS

8.1 ADVERTISING

Contractor shall not publish or use any information concerning this Contract in any format or media for advertising or publicity without prior written consent from the MCC Contract Administrator.

8.2 RETENTION OF RECORDS

The Contractor shall maintain all books, records, documents, data and other evidence relating to this Contract and the provision of materials, supplies, services and/or equipment described herein, including, but not limited to, accounting procedures and practices which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. Contractor shall retain such records for a period of seven (7) years following the date of final payment or as otherwise specified in *Appendix D Specifications*. At no additional cost, these records, including materials generated under the Contract, shall be subject at all reasonable times to inspection, review, or audit by the MCC, personnel duly authorized by the MCC, personnel duly authorized by the Purchaser, the Washington State Auditor's Office, and federal and state officials so authorized by law, regulation or agreement.

If any litigation, claim or audit is started before the expiration of the seven (7) year period, the records shall be retained until final resolution of all litigation, claims, or audit findings involving the records.

8.3 PROPRIETARY OR CONFIDENTIAL INFORMATION

To the extent consistent with Chapter 42.56 RCW, the Public Disclosure Act, the MCC shall maintain the confidentiality of Contractor's information marked confidential or proprietary. If a request is made to view Contractor's proprietary information, the MCC will notify Contractor of the request and of the date that the records will be released to the requester unless Contractor obtains a court order enjoining that disclosure. If Contractor fails to obtain the court order enjoining disclosure, the MCC will release the requested information on the date specified.

The MCC's sole responsibility shall be limited to maintaining the above data in a secure area and to notify Contractor of any request(s) for disclosure for so long as the MCC retains Contractor's information in the MCC records. Failure to so label such materials or failure to timely respond after notice of request for public disclosure has been given shall be deemed a waiver by Contractor of any claim that such materials are exempt from disclosure.

8.4 NON-ENDORSEMENT AND PUBLICITY

Neither the MCC nor the Purchasers/Participating Entities are endorsing the Contractor's Products or Services, nor suggesting that they are the best or only solution to their needs. Contractor agrees to make no reference to the state of Washington, MCC, Purchaser/Participating Entity in any literature, promotional material, brochures, sales presentation or the like, regardless of method of distribution, without the prior review and express written consent of the MCC and/or the impacted Participating Entity.

8.5 PROTECTION OF CONFIDENTIAL AND PERSONAL INFORMATION

Contractor acknowledges that some of the material and information that may come into its possession or knowledge in connection with this Contract or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either Chapter 42.17 RCW or other state or federal statutes ("Confidential Information"). Confidential Information includes, but is not limited to, names, addresses, Social Security numbers, e-mail addresses, telephone numbers, financial profiles, credit card information, driver's license numbers, medical data, law enforcement records, agency source code or object code, agency security data, or information identifiable to an individual that relates to any of these types of information. Contractor agrees to hold Confidential Information in strictest confidence and not to make use of Confidential Information for any purpose other than the performance of this Contract, to release it only to authorized employees or Subcontractors requiring such information for the purposes of carrying out this Contract, and not to release, divulge, publish, transfer, sell, disclose, or otherwise make the information known to any other party without Purchaser's express written consent or as provided by law. Contractor agrees to release such information or material only to employees or Subcontractors who have signed a nondisclosure agreement, the terms of which have been previously approved by Purchaser. Contractor agrees to implement physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information.

"Personal information" including, but not limited to, "Protected Health Information" (PHI) under Health Insurance Portability And Accountability Act (HIPAA), individuals' names, addresses, phone numbers, birth dates, and social security numbers collected, used, or acquired in connection with this Contract shall be protected against unauthorized use, disclosure, modification or loss.

HIPAA establishes national minimum standards for the use and disclosure of certain health information. The Contractor must comply with all HIPAA requirements and rules when determined applicable by the Purchaser. If Purchaser determines that (1) Purchaser is a "covered entity" under HIPAA, and that (2) Contractor will perform "business associate" services and activities covered under HIPAA, then at Purchaser's request, Contractor agrees to execute Purchaser's business associate Contract in compliance with HIPAA.

Contractor shall ensure its directors, officers, employees, Subcontractors or agents use personal information solely for the purposes of accomplishing the services set forth herein. Contractor and its Subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons personal information without the express written consent of the Agency or as otherwise required by law.

Any breach of this provision may result in termination of the Contract and demand for return of all personal information. The Contractor agrees to indemnify and hold harmless the State of Washington and the Purchaser for any damages related to both: (1) the Contractor's unauthorized use of personal information and (2) the unauthorized use of personal information by unauthorized persons as a result of Contractor's failure to sufficiently protect against unauthorized use, disclosure, modification, or loss.

Contractor shall maintain a log documenting the following: the Confidential Information received in the performance of this Contract; the purpose(s) for which the Confidential Information was received; who received, maintained and used the Confidential Information; and the final disposition of the Confidential Information. Contractor's records shall be subject to inspection, review or audit in accordance with Retention of Records.

Purchaser reserves the right to monitor, audit, or investigate the use of Confidential Information collected, used, or acquired by Contractor through this Contract. The monitoring, auditing, or investigating may include, but is not limited to, salting databases.

Violation of this section by Contractor or its Subcontractors may result in termination of this Contract and demand for return of all Confidential Information, monetary damages, or penalties.

Immediately upon expiration or termination of this Contract, Contractor shall, at Purchaser's option: (i) certify to Purchaser that Contractor has destroyed all Confidential Information; or (ii) return all Confidential Information to Purchaser; or (iii) take whatever other steps Purchaser requires of Contractor to protect Purchaser's Confidential Information.

9.0 GENERAL PROVISIONS

9.1 GOVERNING LAW/VENUE

This Contract shall be construed and interpreted in accordance with the laws of the State of Washington, and the venue of any action brought hereunder shall be in the Superior Court for Thurston County.

9.2 SEVERABILITY

If any provision of this Contract or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Contract that can be given effect without the invalid provision, and to this end the provisions of this Contract are declared to be severable.

9.3 SURVIVORSHIP

All transactions executed for Products and Services provided pursuant to the authority of this Contract shall be bound by all of the terms, conditions, Prices and Price discounts set forth herein, notwithstanding the expiration of the initial term of this Contract or any extension thereof. Further, the terms, conditions and warranties contained in this Contract that by their sense and context are intended to survive the completion of the performance, cancellation or termination of this Contract shall so survive. In addition, the terms of the sections titled Overpayments to Contractor; Contractor's Commitments, Warranties and Representations; Protection of Confidential and Personal Information; Order of Precedence, Incorporated Documents, Conflict and Conformity; Non-Endorsement and Publicity; Retention of Records; Proprietary or Confidential Information; Disputes and Remedies; and Limitation of Liability shall survive the termination of this Contract.

9.4 INDEPENDENT STATUS OF CONTRACTOR

In the performance of this Contract, the parties will be acting in their individual, corporate or governmental capacities and not as agents, employees, partners, joint venturers, or associates of one another. The parties intend that an independent contractor relationship will be created by this Contract. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Contractor shall not make any

claim of right, privilege or benefit which would accrue to an employee under Chapter 41.06 RCW, or Title 51 RCW.

9.5 GIFTS AND GRATUITIES

Contractor shall comply with all state laws regarding gifts and gratuities, including but not limited to: RCW 43.19.1937 , RCW 43.19.1939, RCW 42.52.150, RCW 42.52.160, and RCW 42.52.170 under which it is unlawful for any person to directly or indirectly offer, give or accept gifts, gratuities, loans, trips, favors, special discounts, services, or anything of economic value in conjunction with state business or contract activities.

Under RCW 43.19.1937 and the Ethics in Public Service Law, Chapter 42.52 RCW state officers and employees are prohibited from receiving, accepting, taking or seeking gifts (except as permitted by RCW 42.52.150) if the officer or employee participates in contractual matters relating to the purchase of goods or services.

9.6 IMMUNITY AND HOLD HARMLESS

(The following section applies to State of Washington Agencies and Purchasing Cooperative Members only.)

To the fullest extent permitted by law, Contractor shall indemnify, defend and hold harmless State, agencies of State and all officials, agents and employees of State, from and against all claims for injuries, death or damage to property arising out of or resulting from the performance of the contract. Contractor's obligation to indemnify, defend, and hold harmless includes any claim by Contractors' agents, employees, representatives, or any subcontractor or its employees.

Contractor expressly agrees to indemnify, defend, and hold harmless the State for any claim arising out of or incident to Contractor's or any subcontractor's performance or failure to perform the contract. Contractor shall be required to indemnify, defend, and hold harmless the State only to the extent claim is caused in whole or in part by negligent acts or omissions of Contractor.

Contractor waives its immunity under Title 51 to the extent it is required to indemnify, defend and hold harmless State and its agencies, officials, agents or employees.

9.8 NO WAIVER OF SOVEREIGN IMMUNITY

In no event shall this Master Agreement, any Participating Addendum or any contract or any purchase order issued thereunder, or any act of a Lead State or a Participating Entity, be a waiver by the Participating Entity of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

If a claim must be brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for the Participating State. This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

9.9 PERSONAL LIABILITY

It is agreed by and between the parties hereto that in no event shall any official, officer, employee or agent of the State of Washington when executing their official duties in good faith, be in any way

personally liable or responsible for any agreement herein contained whether expressed or implied, nor for any statement or representation made herein or in any connection with this agreement.

9.10 INSURANCE

General Requirements:

Contractor shall, at their own expense, obtain and keep in force insurance as follows until completion of the Contract. Upon request, Contractor shall furnish evidence in the form of a certificate of insurance satisfactory to the State of Washington that insurance, in the following kinds and minimum amounts, has been secured. Failure to provide proof of insurance, as required, will result in Contract cancellation.

Contractor shall include all Subcontractors as insureds under all required insurance policies, or shall furnish separate Certificates of Insurance and endorsements for each Subcontractor. Subcontractor(s) must comply fully with all insurance requirements stated herein. Failure of Subcontractor(s) to comply with insurance requirements does not limit Contractor's liability or responsibility.

All insurance provided in compliance with this Contract shall be primary as to any other insurance or self-insurance programs afforded to or maintained by the state.

Specific Requirements:

Employers Liability (Stop Gap): The Contractor will at all times comply with all applicable workers' compensation, occupational disease, and occupational health and safety laws, statutes, and regulations to the full extent applicable and will maintain Employers Liability insurance with a limit of no less than $1,000,000.00. The State of Washington will not be held responsible in any way for claims filed by the Contractor or their employees for services performed under the terms of this Contract.

Commercial General Liability Insurance: The Contractor shall at all times during the term of this Contract, carry and maintain commercial general liability insurance and if necessary, commercial umbrella insurance for bodily injury and property damage arising out of services provided under this Contract. This insurance shall cover such claims as may be caused by any act, omission, or negligence of the Contractor or its officers, agents, representatives, assigns, or servants.

The insurance shall also cover bodily injury, including disease, illness and death, and property damage arising out of the Contractor's premises/operations, independent Contractors, products/completed operations, personal injury and advertising injury, and contractual liability (including the tort liability of another assumed in a business Contract), and contain separation of insured's (cross liability) conditions.

Contractor waives all rights against the State of Washington for the recovery of damages to the extent they are covered by general liability or umbrella insurance.

The limits of liability insurance shall not be less than as follows:

General Aggregate Limits (other than products-completed operations)	$2,000,000
Products-Completed Operations Aggregate	$2,000,000
Personal and Advertising Injury Aggregate	$1,000,000
Each Occurrence (applies to all of the above)	$1,000,000
Fire Damage Limit (per occurrence)	$ 50,000
Medical Expense Limit (any one person)	$ 5,000

Business Auto Policy (BAP):

In the event that services delivered pursuant to this Contract involve the use of vehicles, or the transportation of clients, automobile liability insurance shall be required. The coverage provided shall protect against claims for bodily injury, including illness, disease, and death; and property damage caused by an occurrence arising out of or in consequence of the performance of this service by the Contractor, Subcontractor, or anyone employed by either.

Contractor shall maintain business auto liability and, if necessary, commercial umbrella liability insurance with a combined single limit not less than $1,000,000 per occurrence. The business auto liability shall include Hired and Non-Owned coverage.

Contractor waives all rights against the State of Washington for the recovery of damages to the extent they are covered by business auto liability or commercial umbrella liability insurance.

Additional Insurance Provisions:

All above insurance policies shall include, but not be limited to, the following provisions:

Additional Insured:

The State of Washington and all authorized Purchasers shall be named as an additional insured on all general liability, umbrella, excess, and property insurance policies. All policies shall be primary over any other valid and collectable insurance.

Notice of Policy(ies) Cancellation/Non-renewal:

For insurers subject to Chapter 48.18 RCW (Admitted and regulated by the Washington State Insurance Commissioner) a written notice shall be given to the director of purchasing or designee forty-five (45) calendar days prior to cancellation or any material change to the policy(ies) as it relates to this Contract. Written notice shall include the affected Contract reference number.

Surplus Lines:

For insurers subject to Chapter 48.15 RCW (Surplus Lines) a written notice shall be given to the director of purchasing or designee twenty (20) calendar days prior to cancellation or any material change to the policy(ies) as it relates to this Contract. Written notice shall include the affected Contract reference number.

Cancellation for Non-payment to Premium:

If cancellation on any policy is due to non-payment of premium, a written notice shall be given the director of purchasing or designee ten (10) calendar days prior to cancellation. Written notice shall include the affected Contract reference number.

Identification:

Policy(ies) and Certificates of Insurance shall include the affected Contract reference number.

Insurance Carrier Rating:

The insurance required above shall be issued by an insurance company authorized to do business within the State of Washington. Insurance is to be placed with a carrier that has a rating of A- Class VII or better in the most recently published edition of Best's Reports. Any exception must be reviewed and approved by the Risk Manager for the State of Washington, by submitting a copy of the Contract and evidence of insurance before Contract commencement. If an insurer is not admitted, all insurance policies and procedures for issuing the insurance policies must comply with Chapter 48.15 RCW and Chapter 284-15 WAC .

Excess Coverage:

The limits of all insurance required to be provided by the Contractor shall be no less than the minimum amounts specified. However, coverage in the amounts of these minimum limits shall not be construed to relieve the Contractor from liability in excess of such limits.

Limit Adjustments:

The state reserves the right to increase or decrease limits as appropriate.

9.11 INDUSTRIAL INSURANCE COVERAGE

The Contractor shall comply with the provisions of Title 51 RCW Industrial Insurance. If the Contractor fails to provide industrial insurance coverage or fails to pay premiums or penalties on behalf of its employees as may be required by law, the MCC may terminate this Contract. This provision does not waive any of the Washington State Department of Labor and Industries (L&I) rights to collect from the Contractor.

9.12 NONDISCRIMINATION

During the performance of this Contract, the Contractor shall comply with all applicable federal and state nondiscrimination laws, regulations and policies, including, but not limited to, Title VII of the Civil Rights Act, 42 U.S.C. section 12101 et. seq.; the Americans with Disabilities Act (ADA); and, Chapter 49.60 RCW, Discrimination – Human Rights Commission.

9.13 OSHA AND WISHA REQUIREMENTS

Contractor agrees to comply with conditions of the Federal Occupational Safety and Health Administration (OSHA) and, if manufactured or stored in the State of Washington, the Washington Industrial Safety and Health Act (WISHA) and the standards and regulations issued there under, and certifies that all items furnished and purchased will conform to and comply with said laws, standards and regulations. Contractor further agrees to indemnify and hold harmless MCC and Purchaser from all damages assessed against Purchaser as a result of Contractor's failure to comply with those laws, standards and regulations, and for the failure of the items furnished under the Contract to so comply.

9.14 ANTITRUST

The state maintains that, in actual practice, overcharges resulting from antitrust violations are borne by the Purchaser. Therefore, the Contractor hereby assigns to the State of Washington any and all of the Contractor's claims for such price fixing or overcharges which arise under federal or state antitrust laws, relating to the materials, supplies, services and/or equipment purchased under this Contract.

9.15 WAIVER

Failure or delay of the MCC or Purchaser to insist upon the strict performance of any term or condition of the Contract or to exercise any right or remedy provided in the Contract or by law; or the MCC's or Purchaser's acceptance of or payment for materials, supplies, services and/or equipment, shall not release the Contractor from any responsibilities or obligations imposed by this Contract or by law, and shall not be deemed a waiver of any right of the MCC or Purchaser to insist upon the strict performance of the entire agreement by the Contractor. In the event of any claim for breach of Contract against the Contractor, no provision of this Contract shall be construed, expressly or by implication, as a waiver by the MCC or Purchaser of any existing or future right and/or remedy available by law.

9.16 APPLICABLE STANDARD TERMS AND CONDITIONS

Appendix B titled: *(WSCA-NASPO) Master Agreement Standard Terms and Conditions*, shall supplement the terms and conditions appearing elsewhere within this contract.

10.0 DISPUTES AND REMEDIES

10.1 PROBLEM RESOLUTION AND DISPUTES

Problems arising out of the performance of this Contract shall be resolved in a timely manner at the lowest possible level with authority to resolve such problem. If a problem persists and cannot be resolved, it may be escalated within each organization.

In the event a bona fide dispute concerning a question of fact arises between MCC or the Purchaser and Contractor and it cannot be resolved between the parties through the normal escalation processes, either party may initiate the dispute resolution procedure provided herein.

The initiating party shall reduce its description of the dispute to writing and deliver it to the responding party. The responding party shall respond in writing within three (3) Business Days. The initiating party shall have three (3) Business Days to review the response. If after this review a resolution cannot be reached, both parties shall have three (3) Business Days to negotiate in good faith to resolve the dispute.

If the dispute cannot be resolved after three (3) Business Days, a Dispute Resolution Panel may be requested in writing by either party who shall also identify the first panel member. Within three (3) Business Days of receipt of the request, the other party will designate a panel member. Those two panel members will appoint a third individual to the Dispute Resolution Panel within the next three (3) Business Days.

The Dispute Resolution Panel will review the written descriptions of the dispute, gather additional information as needed, and render a decision on the dispute in the shortest practical time.

Each party shall bear the cost for its panel member and share equally the cost of the third panel member.

Both parties agree to exercise good faith in dispute resolution and to settle disputes prior to using a Dispute Resolution Panel whenever possible.

Unless irreparable harm will result, neither party shall commence litigation against the other before the Dispute Resolution Panel has issued its decision on the matter in dispute.

MCC, the Purchaser and Contractor agree that, the existence of a dispute notwithstanding, they will continue without delay to carry out all their respective responsibilities under this Contract that are not affected by the dispute.

If the subject of the dispute is the amount due and payable by Purchaser for materials, supplies, services and/or equipment being provided by Contractor, Contractor shall continue providing materials, supplies, services and/or equipment pending resolution of the dispute provided Purchaser pays Contractor the amount Purchaser, in good faith, believes is due and payable, and places in escrow the difference between such amount and the amount Contractor, in good faith, believes is due and payable.

10.2 ADMINISTRATIVE SUSPENSION

When it is in the best interest of the state, the MCC may at any time, and without cause, suspend the Contract or any portion thereof for a period of not more than thirty (30) calendar days per event by written notice from the Contract Administrator to the Contractor's Representative. Contractor shall

resume performance on the next business day following the 30th day of suspension unless an earlier resumption date is specified in the notice of suspension. If no resumption date was specified in the notice of suspension, the Contractor can be demanded and required to resume performance within the 30 day suspension period by the Contract Administrator providing the Contractor's Representative with written notice of such demand.

10.3 FORCE MAJEURE

The term "force majeure" means an occurrence that causes a delay that is beyond the control of the party affected and could not have been avoided by exercising reasonable diligence. Force majeure shall include acts of God, war, riots, strikes, fire, floods, epidemics, or other similar occurrences.

Exceptions: Except for payment of sums due, neither party shall be liable to the other or deemed in breach under this Contract if, and to the extent that, such party's performance of this Contract is prevented by reason of force majeure.

Notification: If either party is delayed by force majeure, said party shall provide written notification within forty-eight (48) hours. The notification shall provide evidence of the force majeure to the satisfaction of the other party. Such delay shall cease as soon as practicable and written notification of same shall likewise be provided. So far as consistent with the Rights Reserved below, the time of completion shall be extended by Contract amendment for a period of time equal to the time that the results or effects of such delay prevented the delayed party from performing in accordance with this Contract.

Rights Reserved: The MCC reserves the right to authorize an amendment to this Contract, terminate the Contract, and/or purchase materials, supplies, equipment and/or services from the best available source during the time of force majeure, and Contractor shall have no recourse against the Purchaser or Participating Entity.

10.4 ALTERNATIVE DISPUTE RESOLUTION FEES AND COSTS

In the event that the parties engage in arbitration, mediation or any other alternative dispute resolution forum to resolve a dispute in lieu of litigation, both parties shall share equally in the cost of the alternative dispute resolution method, including cost of mediator or arbitrator. In addition, each party shall be responsible for its own attorneys' fees incurred as a result of the alternative dispute resolution method.

10.5 NON-EXCLUSIVE REMEDIES

The remedies provided for in this Contract shall not be exclusive but are in addition to all other remedies available under law.

10.6 LIMITATION OF LIABILITY

The parties agree that neither Contractor, MCC nor Purchaser shall be liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages except a claim related to bodily injury or death, or a claim or demand based on patent, copyright, or other intellectual property right infringement, in which case liability shall be as set forth elsewhere in this Contract. This section does not modify any sections regarding liquidated damages or any other conditions as are elsewhere agreed to herein between the parties. The damages specified in the sections titled Termination for Default and Retention of Records are not consequential, incidental, indirect, or special damages as that term is used in this section.

Neither the Contractor, the MCC nor Purchaser shall be liable for damages arising from causes beyond the reasonable control and without the fault or negligence of the Contractor, the MCC or

Purchaser. Such causes may include, but are not restricted to, acts of God or of the public enemy, acts of a governmental body other than the MCC or the Purchaser acting in either its sovereign or contractual capacity, war, explosions, fires, floods, earthquakes, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the delays must be beyond the reasonable control and without fault or negligence of the Contractor, the MCC or the Purchaser, or their respective Subcontractors.

If delays are caused by a Subcontractor without its fault or negligence, Contractor shall not be liable for damages for such delays, unless the Services to be performed were obtainable on comparable terms from other sources in sufficient time to permit Contractor to meet its required performance schedule.

Neither party shall be liable for personal injury to the other party or damage to the other party's property except personal injury or damage to property proximately caused by such party's respective fault or negligence.

10.7 FEDERAL FUNDING

In the event that a federally funded acquisition results from this procurement, the Contractor may be required to provide additional information (free of charge) at the request of the MCC or Purchaser. Further, the Contractor may be subject to those federal requirements specific to the commodity.

10.8 FEDERAL RESTRICTIONS ON LOBBYING

Contractor certifies that under the requirements of Lobbying Disclosure Act, 2 U.S.C., Section 1601 et seq., no Federal appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

10.9 FEDERAL DEBARMENT AND SUSPENSION

The Contractor certifies, that neither it nor its "principals" (as defined in 49 CFR. 29.105 (p) is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

11.0 CONTRACT TERMINATION

11.1 MATERIAL BREACH

A Contractor may be Terminated for Cause by the MCC, at the sole discretion of the Contract Administrator, for failing to perform a contractual requirement or for a material breach of any term or condition. Material breach of a term or condition of the Contract may include but is not limited to:

1. Contractor failure to perform services or deliver materials, supplies, or equipment by the date required or by an alternate date as mutually agreed in a written amendment to the Contract;
2. Contractor failure to carry out any warranty or fails to perform or comply with any mandatory provision of the contract;

3. Contractor becomes insolvent or in an unsound financial condition so as to endanger performance hereunder;
4. Contractor becomes the subject of any proceeding under any law relating to bankruptcy, insolvency or reorganization, or relief from creditors and/or debtors that endangers the Contractor's proper performance hereunder;
5. Appointment of any receiver, trustee, or similar official for Contractor or any of the Contractor's property and such appointment endangers the Contractor's proper performance hereunder;
6. A determination that the Contractor is in violation of federal, state, or local laws or regulations and that such determination renders the Contractor unable to perform any aspect of the Contract.

11.2 OPPORTUNITY TO CURE

In the event that Contractor fails to perform a contractual requirement or materially breaches any term or condition, the MCC may issue a written cure notice. The Contractor may have a period of time in which to cure. The MCC is not required to allow the Contractor to cure defects if the opportunity for cure is not feasible as determined solely within the discretion of the MCC. Time allowed for cure shall not diminish or eliminate Contractor's liability for liquidated or other damages, or otherwise affects any other remedies available against Contractor under the Contract or by law.

If the breach remains after Contractor has been provided the opportunity to cure, the MCC may do any one or more of the following:

1. Exercise any remedy provided by law;
2. Terminate this Contract and any related Contracts or portions thereof;
3. Procure replacements and impose damages as set forth elsewhere in this Contract;
4. Impose actual or liquidated damages;
5. Suspend or bar Contractor from receiving future Solicitations or other opportunities;
6. Require Contractor to reimburse the state for any loss or additional expense incurred as a result of default or failure to satisfactorily perform the terms of the Contract.

11.3 TERMINATION FOR CAUSE

In the event the Contract Administrator, in its sole discretion, determines that the Contractor has failed to comply with the conditions of this Contract in a timely manner or is in material breach, the Contract Administrator has the right to suspend or terminate this Contract, in part or in whole. The Contract Administrator shall notify the Contractor in writing of the need to take corrective action. If corrective action is not taken within thirty (30) calendar days or as otherwise specified by the Contract Administrator, or if such corrective action is deemed by the Contract Administrator to be insufficient, the Contract may be terminated. The Contract Administrator reserves the right to suspend all or part of the Contract, withhold further payments, or prohibit the Contractor from incurring additional obligations of funds during investigation of the alleged breach and pending corrective action by the Contractor or a decision by the Contract Administrator to terminate the Contract.

In the event of termination, the MCC shall have the right to procure for all Purchasers any replacement materials, supplies, services and/or equipment that are the subject of this Contract on

the open market. In addition, the Contractor shall be liable for damages as authorized by law including, but not limited to, any price difference between the original contract and the replacement or cover contract and all administrative costs directly related to the replacement contract, e.g., cost of the competitive bidding, mailing, advertising and staff time.

If it is determined that: (1) the Contractor was not in material breach; or (2) failure to perform was outside of Contractor's or its Subcontractor's control, fault or negligence, the termination shall be deemed to be a "Termination for Convenience". The rights and remedies of the MCC and/or the Purchaser provided in this Contract are not exclusive and are in addition to any other rights and remedies provided by law.

11.4 TERMINATION FOR CONVENIENCE

Except as otherwise provided in this Contract, the MCC, at the sole discretion of the Contract Administrator, may terminate this Contract, in whole or in part by giving thirty (30) calendar days written notice beginning on the second day after mailing to the Contractor. If this Contract is so terminated, Purchasers shall be liable only for payment required under this Contract for properly authorized services rendered, or materials, supplies and/or equipment delivered to and Accepted by the Purchaser prior to the effective date of Contract termination. Neither the MCC nor the Purchaser shall have any other obligation whatsoever to the Contractor for such termination. This Termination for Convenience clause may be invoked by the MCC when it is in the best interest of the State of Washington and/or WSCA-NASPO.

11.5 TERMINATION FOR WITHDRAWAL OF AUTHORITY

In the event that the MCC and/or Purchaser's authority to perform any of its duties is withdrawn, reduced, or limited in any way after the commencement of this Contract and prior to normal completion, the MCC may terminate this Contract, in whole or in part, by thirty (30) calendar days written notice to Contractor.

11.6 TERMINATION FOR NON-ALLOCATION OF FUNDS

If funds are not allocated to Purchaser(s) to continue this Contract in any future period, MCC may terminate this Contract by thirty (30) calendar days written notice to Contractor or work with Contractor to arrive at a mutually acceptable resolution of the situation. Purchaser will not be obligated to pay any further charges for materials, supplies, services and/or equipment including the net remainder of agreed to consecutive periodic payments remaining unpaid beyond the end of the then-current period. MCC and/or Purchaser agrees to notify Contractor in writing of such non-allocation at the earliest possible time.

No penalty shall accrue to the Purchaser in the event this section shall be exercised. This section shall not be construed to permit MCC to terminate this Contract in order to acquire similar materials, supplies, services and/or equipment from a third party.

11.7 TERMINATION FOR CONFLICT OF INTEREST

MCC may terminate this Contract by written notice to Contractor if it is determined, after due notice and examination, that any party to this Contract has violated Chapter 42.52 RCW , Ethics in Public Service, or any other laws regarding ethics in public acquisitions and procurement and performance of contracts. In the event this Contract is so terminated, the MCC and /or Purchaser shall be entitled to pursue the same remedies against Contractor as it could pursue in the event that the Contractor breaches this Contract.

11.8 TERMINATION BY MUTUAL AGREEMENT

The MCC and the Contractor may terminate this Contract in whole or in part, at any time, by mutual agreement.

11.9 TERMINATION PROCEDURE

In addition to the procedures set forth below, if the MCC terminates this Contract, Contractor shall follow any procedures the Contract Administrator specifies in the termination notice.

Upon termination of this Contract and in addition to any other rights provided in this Contract, Contract Administrator may require the Contractor to deliver to the Purchaser any property specifically produced or acquired for the performance of such part of this contract as has been terminated. The provisions of the "Treatment of Assets" clause shall apply in such property transfer.

The Purchaser shall pay to the Contractor the agreed upon price, if separately stated, for completed work and service(s) Accepted by the Purchaser, and the amount agreed upon by the Contractor and the Purchaser for (i) completed materials, supplies, services rendered and/or equipment for which no separate price is stated, (ii) partially completed materials, supplies, services rendered and/or equipment, (iii) other materials, supplies, services rendered and/or equipment which are Accepted by the Purchaser, and (iv) the protection and preservation of property, unless the termination is for cause, in which case the MCC and the Purchaser shall determine the extent of the liability of the Purchaser. Failure to agree with such determination shall be a dispute within the meaning of the "Disputes" clause of this contract. The Purchaser may withhold from any amounts due the Contractor such sum as the Contract Administrator and Purchaser determine to be necessary to protect the Purchaser against potential loss or liability.

The rights and remedies of the MCC and/or the Purchaser provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this contract.

After receipt of a termination notice, and except as otherwise expressly directed in writing by the Contract Administrator, the Contractor shall:

1. Stop all work, order fulfillment, shipments, and deliveries under the Contract on the date, and to the extent specified, in the notice;
2. Place no further orders or subcontracts for materials, services, supplies, equipment and/or facilities in relation to the Contract except as is necessary to complete or fulfill such portion of the Contract that is not terminated;
3. Complete or fulfill such portion of the Contract that is not terminated in compliance with all contractual requirements;
4. Assign to the Purchaser, in the manner, at the times, and to the extent directed by the Contract Administrator on behalf of the Purchaser, all of the rights, title, and interest of the Contractor under the orders and subcontracts so terminated, in which case the Purchaser has the right, at its discretion, to settle or pay any or all claims arising out of the termination of such orders and subcontracts;
5. Settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the Contract Administrator and/or the Purchaser to the extent Contract Administrator and/or the Purchaser may require, which approval or ratification shall be final for all the purposes of this clause;

6. Transfer title to the Purchaser and deliver in the manner, at the times, and to the extent directed by the Contract Administrator on behalf of the Purchaser any property which, if the Contract had been completed, would have been required to be furnished to the Purchaser;
7. Take such action as may be necessary, or as the Contract Administrator and/or the Purchaser may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the MCC and/or the Purchaser has or may acquire an interest.

12.0 CONTRACT EXECUTION

12.1 PARTIES

This Contract ("Contract") is entered into by and between the state of Washington, acting by and through the Department of Enterprise Services, Master Contracts & Consulting (MCC), an agency of Washington State government ("MCC" or "State") located at 1500 Jefferson Street SE, Olympia WA 98501, and Sentinel Offender Services, LLC, a Limited Liability Company (LLC) licensed to conduct business in the state of Washington ("Contractor"), located at 201 Technology Drive, Irvine, California 92618 for the purpose of providing products and services for the electronic monitoring of offenders.

12.2 ENTIRE AGREEMENT

This Contract document and all subsequently issued amendments comprise the entire agreement between the MCC and the Contractor. No other statements or representations, written or oral, shall be deemed a part of the Contract.

This Contract sets forth the entire agreement between the parties with respect to the subject matter hereof and except as provided in the section titled **Contractor Commitments, Warranties and Representations**, understandings, agreements, representations, or warranties not contained in this Contract or a written amendment hereto shall not be binding on either party. Except as provided herein, no alteration of any of the terms, conditions, delivery, Price, quality, or Specifications of this Contract will be effective without the written consent of both parties.

12.3 ORDER OF PRECEDENCE, INCORPORATED DOCUMENTS, CONFLICT AND CONFORMITY

Incorporated Documents:

Each of the documents listed below is, by this reference, incorporated into this Contract as though fully set forth herein.

1. The MCC's Solicitation document #00212 with all attachments and exhibits, and all amendments thereto
2. Contractor's response to the Solicitation #00212;
3. A Participating Entity's Participating Addendum ("PA");
4. The terms and conditions contained on Purchaser's Order Documents, if used; and
5. All Contractor or manufacturer publications, written materials and schedules, charts, diagrams, tables, descriptions, other written representations and any other supporting materials Contractor made available to Purchaser and used to affect the sale of the Product and /or Service to the Purchaser.

Order of Precedence:

In the event of a conflict in such terms, or between the terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

1. Applicable Federal statutes and regulations.
2. A Participating Entity's Participating Addendum ("PA").
3. Mutually agreed written amendments to this Contract.
4. This Contract Number 00212.
5. The Statement of Work or Work Order.
6. The MCC's Solicitation document with all attachments and exhibits, and all amendments thereto.
7. Contractor's response to the Solicitation.
8. Any other provision, term, or materials incorporated into the Contract by reference.

Conflict: To the extent possible, the terms of this Contract shall be read consistently.

Conformity: If any provision of this Contract violates any Federal or State of Washington statute or rule of law, it is considered modified to conform to that statute or rule of law.

12.4 LEGAL NOTICES

Any notice or demand or other communication required or permitted to be given under this Contract or applicable law (except notice of malfunctioning Equipment) shall be effective only if it is in writing and signed by the applicable party, properly addressed, and either delivered in person, or by a recognized courier service, or deposited with the United States Postal Service as first-class mail, (postage prepaid),), via facsimile or by electronic mail, to the parties at the addresses, fax numbers, or e-mail addresses provided in this section. For purposes of complying with any provision in this Contract or applicable law that requires a "writing," such communication, when digitally signed with a Washington State Licensed Certificate, shall be considered to be "in writing" or "written" to an extent no less than if it were in paper form.

To Contractor at:	**To MCC at:**
Sentinel Offender Services, LLC	State of Washington Department of Enterprise Services Master Contracts & Consulting
Attn: Leo Carson, Vice President of Strategic Sales	**Attn:** MCC Contract Administrator
201 Technology Drive Irvine, California 92618	Mail: Post Office Box 41411 Olympia, Washington 98504-1411 Street: 1500 Jefferson Street, SE Olympia, WA 98501
Phone: (888) 843-5590	Phone: (360) 407-9430
Fax: (800) 327-1178	Fax: (360) 586-2426
E-mail: leo.carson@sentrak.com	E-mail: robert.paulson@des.wa.gov

Notices shall be effective upon receipt or four (4) Business Days after mailing, whichever is earlier. The notice address as provided herein may be changed by written notice given as provided above.

In the event that a subpoena or other legal process commenced by a third party in any way concerning the Equipment or Services provided pursuant to this Contract is served upon Contractor or MCC, such party agrees to notify the other party in the most expeditious fashion possible following receipt of such subpoena or other legal process. Contractor and MCC further agree to cooperate with the other party in any lawful effort by the other party to contest the legal validity of such subpoena or other legal process commenced by a third party.

12.5 LIENS, CLAIMS AND ENCUMBRANCES

All materials, equipment, supplies and/or services shall be free of all liens, claims, or encumbrances of any kind, and if the MCC or the Purchaser requests, a formal release of same shall be delivered to the respective requestor.

12.6 AUTHORITY TO BIND

The signatories to this Contract represent that they have the authority to bind their respective organizations to this Contract.

12.7 COUNTERPARTS

This Contract may be executed in counterparts or in duplicate originals. Each counterpart or each duplicate shall be deemed an original copy of this Contract signed by each party, for all purposes.

SIGNATURES

In Witness Whereof, the parties hereto, having read this Contract in its entirety, including all attachments, do agree in each and every particular and have thus set their hands hereunto.

This Contract is effective May 1, 2013, or the date of last signature whichever is later.
This is a Partial award for: <u>Contract 00212</u>

Approved (Lead State)		**Approved**
State of Washington Department of Enterprise Services Master Contracts & Consulting 1500 Jefferson Street, SE Olympia, WA 98501		Sentinel Offender Services, LLC 201 Technology Drive Irvine, California 92618
/s/ 6-3-13 Signature Date		/s/ May 3, 2013 Signature Date
Robert Paulson, Jr., C.P.M. Print or Type Name		Hans Kintsch Print or Type Name
Contract Administrator Title		Chief Financial Officer Title
/s/ 6-3-13 Signature Date		
Dale Colbert, CPPO Print or Type Name		
Unit Manager Title		

/s/	6/4/13
Signature	Date
Christine Warnock, CPPO	
Print or Type Name	
Chief Procurement Officer	
Title	

APPENDIX A STANDARD DEFINITIONS

This section contains definitions of terms commonly used in Solicitations conducted by the State of Washington, Master Contracts & Consulting. Additional definitions may also be found in Chapter 43.19 RCW and WAC 200-300-015, and all terms contained herein will be read consistently with those definitions.

Acceptance	The materials, supplies, services, and/or equipment have passed appropriate Inspection. In the event that there is a formal Acceptance Testing period required in the Solicitation document then acceptance is formalized in writing. If there is no Acceptance Testing, acceptance may occur when the Products are delivered and inspected.
Acceptance Testing	The process for ascertaining that the materials, supplies, services, and/or equipment meets the standards set forth in the Solicitation, prior to Acceptance by the Purchaser.
Agency	Includes State of Washington institutions, the offices of the elective state officers, the Supreme Court, the court of appeals, the administrative and other departments of state government, and the offices of all appointive officers of the state. In addition, colleges, community colleges, and universities who choose to participate in State Contract(s) are included. "Agency" does not include the legislature.
All or Nothing	The result of a competitive Solicitation that requires that a Contract be executed with a single Bidder for delivery of goods and/or services. In the event that suppliers are unable to deliver the entirety of the goods and/or services required, no Contract is executed. No partial fulfillment opportunities are available as a result of the Solicitation. A method of award resulting from a competitive Solicitation by which the MCC will award the resulting Contract to a single Bidder. Also, a designation the Bidder may use in its Bid or Response to indicate its offer is contingent upon full award and it will not accept a partial award.
Alternate	A substitute offer of materials, supplies, services and/or equipment that is not at least a functional Equal in features, performance and use and which materially deviates from one or more of the specifications in a competitive Solicitation.
Amendment	A change to a legal document. For the purposes of a Solicitation document, an amendment shall be a unilateral change issued by the MCC, at its sole discretion.
Authorized Representative	An individual designated by the Bidder or Contractor to act on its behalf and with the authority to legally bind the Bidder or Contractor concerning the terms and conditions set forth in Solicitation, Bid and Contract documents.
Bid	A sealed written offer to perform a Contract to provide materials, supplies, services, and/or equipment in reply to an Invitation For Bid (IFB).
Bidder	A Vendor who submits a Bid or Proposal in reply to a Solicitation.
Business Days	Monday through Friday, 8:00 a.m. to 5:00 p.m., Pacific Time, except for holidays observed by the state of Washington.
Calendar Days	Consecutive days of the year including weekends and holidays, each of which commence at 12:00:01 a.m. and end at Midnight, Pacific Time. When “days” are not specified, Calendar Days shall prevail.

Contract	An agreement, or mutual assent, between two or more competent parties with the elements of the agreement being offer, acceptance, and consideration.
Contract Administrator	The person designated to manage the resultant Contract for the MCC. The primary contact for the MCC with Purchasers and Contractor on a specific Contract.
Contractor	Individual, company, corporation, firm, or combination thereof with whom the MCC develops a Contract for the procurement of materials, supplies, services, and/or equipment. It shall also include any Subcontractor retained by Contractor as permitted under the terms of the Contract.
Equal	An offer of materials, supplies, services and/or equipment that meets or exceeds the quality, performance and use of the specifications identified in a Solicitation.
Estimated Useful Life	The estimated time from the date of acquisition to the date of replacement or disposal, determined in any reasonable manner.
Inspection	An examination of delivered material, supplies, services, and/or equipment prior to Acceptance aimed at forming a judgment as to whether such delivered items are what was ordered, were properly delivered and ready for Acceptance. Inspection may include a high level visual examination or a more thorough detailed examination as is customary to the type of purchase, as set forth in the solicitation document and/or as agreed between the parties. Inspection shall be acknowledged by an authorized signature of the Purchaser.
Invitation For Bid (IFB)	The form utilized to solicit Bids in the formal, sealed Bid procedure and any amendments thereto issued in writing by the MCC. Specifications and qualifications are clearly defined.
Lead Time/After Receipt Of Order (ARO)	The period of time between when the Contractor receives the order and the Purchaser receives the materials, supplies, equipment, or services order.
Life Cycle Cost	The total cost of an item to the state over its Estimated Useful Life, including costs of selection, acquisition, operation, maintenance, and where applicable, disposal, as far as these costs can reasonably be determined, minus the salvage value at the end of its estimated useful life.
Master Contracts & Consulting (MCC)	The MCC within the Washington Department of Enterprise Services, Master Contracts & Consulting authorized under Chapter 39.26 RCW (formerly Chapter 43.19 RCW) to develop and administer contracts for goods and services on behalf of state agencies, colleges and universities, non-profit organizations and local governments.
Order Document	A written communication, submitted by a Purchaser to the Contractor, which details the specific transactional elements required by the Purchaser within the scope of the Contract such as delivery date, size, color, capacity, etc. An Order Document may include, but is not limited to field orders, purchase orders, work order or other writings as may be designated by the parties hereto. No additional or alternate terms and conditions on such written communication shall apply unless authorized by the Contract and expressly agreed between the Purchaser and the Contractor.
Procurement Coordinator	The individual authorized by the MCC who is responsible for conducting a specific Solicitation.

Product	Materials, supplies, services, and/or equipment provided under the terms and conditions of this Contract.
Proposal	A sealed written offer to perform a Contract to supply materials, supplies, services, and/or equipment in reply to a Request For Proposal (RFP).
Purchaser	The authorized user of the Contract, as identified in the Solicitation, who may or actually does make purchases of material, supplies, services, and/or equipment under the resulting Contract.
Recycled Material	Waste materials and by-products that have been recovered or diverted from solid waste and that can be utilized in place of a raw or virgin material in manufacturing a product and consists of materials derived from post-consumer waste, manufacturing waste, industrial scrap, agricultural wastes and other items, all of which can be used in the manufacture of new or recycled products.
Recycled Content Product	A product containing recycled material.
Request For Proposal (RFP)	The form utilized to solicit Proposals in the formal, sealed Bid procedure and any amendments thereto issued in writing by the MCC. The specifications and qualification requirements are written in an outcome based form allowing for consideration of a broad range of different solutions to meet the procurement need.
Responsible	The ability, capacity, and skill to perform the Contract or provide the service required , including, but not limited to the character, integrity, reputation, judgment, experience, and efficiency of the Bidder; Further considerations may include, but are not limited to whether the Bidder can perform the contract within the time specified, the quality of performance of previous contracts or services, the previous and existing compliance by the Bidder with laws relating to the contract or services and such other information as may be secured having a bearing on the decision to award the contract:
Responsive	A Bid or Proposal that meets all material terms of the Solicitation document.
Response	A Bid or Proposal
Solicitation	The process of notifying prospective Bidders that the MCC desires to receive competitive Bids or Proposals for furnishing specified materials, supplies, services, and/or equipment. Also includes reference to the actual documents used for that process, including: the Invitation For Bids (IFB) or Request For Proposals (RFP), along with all attachments and exhibits thereto.
State	The State of Washington acting by and through the MCC.

State Contract	The written document memorializing the agreement between the successful Bidder and the MCC for materials, supplies, services, and/or equipment and/or administered by the Master Contracts & Consulting on behalf of the State of Washington. "State Contract" does not include the following: • Colleges and universities that choose to purchase under RCW 28B.10.029 • Purchases made in accordance with state purchasing policy under Washington Purchasing Manual Part 6.11 Best Buy Program; • Purchases made pursuant to authority granted or delegated under RCW 43.19.190(2) or (3) • Purchases authorized as an emergency purchase under RCW 43.19.200(2); or • Purchases made pursuant to other statutes granting the Agency authority to independently conduct purchases of materials, supplies, services, or equipment.
Subcontractor	A person or business that is, or will be, providing or performing an essential aspect of the Contract under the direction and responsibility of the Contractor and with the agreement of the MCC.
Vendor	A provider of materials, supplies, services, and/or equipment.
Washington's Electronic Business Solution (WEBS)	The Vendor registration and Bidder notification system maintained by the Washington State Department of Enterprise Services located at: www.ga.wa.gov/webs.

APPENDIX B WSCA-NASPO MASTER AGREEMENT STANDARD TERMS AND CONDITIONS

1. RESERVED.

2. AMENDMENTS. The terms of this contract shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the WSCA-NASPO Contract Administrator.

3. ASSIGNMENT/SUBCONTRACT. Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this contract, in whole or in part, without the prior written approval of the WSCA-NASPO Contract Administrator.

4. CANCELLATION. Unless otherwise stated in the special terms and conditions, any contract entered into as a result of this bid may be canceled by either party upon 60 days notice, in writing, prior to the effective date of the cancellation. Further, any Participating State may cancel its participation upon 30 days written notice, unless otherwise limited or stated in the special terms and conditions of this solicitation. Cancellation may be in whole or in part. Any cancellation under this provision shall not effect the rights and obligations attending orders outstanding at the time of cancellation, including any right of and Purchasing Entity to indemnification by the Contractor, rights of payment for goods/services delivered and accepted, and rights attending any warranty or default in performance in association with any order. Cancellation of the contract due to Contractor default may be immediate.

5. CONFIDENTIALITY, NON-DISCLOSURE AND INJUNCTIVE RELIEF.
5.1 Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing the Product under this Master Agreement, be exposed to or acquire information that is confidential to Participating Entity or Participating Entity's clients. Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (a) any Participating Entity records, (b) personnel records, and (c) information concerning individuals, is confidential information of Participating Entity ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (a) is or becomes (other than by disclosure by Contractor) publicly known; (b) is furnished by Participating Entity to others without restrictions similar to those imposed by this Master Agreement; (c) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (d) is obtained from a source other than Participating Entity without the obligation of confidentiality, (e) is disclosed with the written consent of Participating Entity or; (f) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

5.2 Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than the performance of this Master Agreement to Participating Entity hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Participating Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Participating Entity immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement and Contractor shall at its expense cooperate with Participating Entity in seeking injunctive or other equitable relief in the name of Participating Entity or Contractor against any such person. Except as directed by Participating Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Participating Entity's request, Contractor shall turn over to Participating Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

5.3 Injunctive Relief. Contractor acknowledges that breach of this Section, including disclosure of any Confidential Information, will cause irreparable injury to Participating Entity that is inadequately compensable in damages. Accordingly, Participating Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Participating Entity and are reasonable in scope and content.

6. DEBARMENT. The contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. If the contractor cannot certify this statement, attach a written explanation for review by WSCA-NASPO.

7. DEFAULTS & REMEDIES.

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

i. Nonperformance of contractual requirements; or

ii. A material breach of any term or condition of this Master Agreement; or

iii. Any representation or warranty by Contractor in response to the solicitation or in this Master Agreement proves to be untrue or materially misleading; or

iv. Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

v. Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 15 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time

allowed for cure shall not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

i. Exercise any remedy provided by law; and

ii. Terminate this Master Agreement and any related Contracts or portions thereof; and

iii. Impose liquidated damages as provided in this Master Agreement; and

iv. Suspend Contractor from receiving future bid solicitations; and

v. Suspend Contractor's performance; and

vi. Withhold payment until the default is remedied.

d. In the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum.

8. DELIVERY. Unless otherwise indicated in the Master Agreement, the prices are the delivered price to any Participating State agency or political subdivision. All deliveries shall be F.O.B. destination with all transportation and handling charges paid by the contractor. Responsibility and liability for loss or damage shall remain the Contractor until final inspection and acceptance when responsibility shall pass to the Buyer except as to latent defects, fraud and Contractor's warranty obligations. The minimum shipment amount will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an order to be shipped without transportation charges that is back ordered shall be shipped without charge.

9. FORCE MAJEURE. Neither party to this contract shall be held responsible for delay or default caused by fire, riot, acts of God and/or war which is beyond that party's reasonable control. WSCA-NASPO may terminate this contract after determining such delay or default will reasonably prevent successful performance of the contract.

10. GOVERNING LAW. This procurement and the resulting agreement shall be governed by and construed in accordance with the laws of the state sponsoring and administering the procurement. The construction and effect of any Participating Addendum or order against the contract(s) shall be governed by and construed in accordance with the laws of the Participating Entity's State. Venue for any claim, dispute or action concerning an order placed against the contract(s) or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

11. INDEMNIFICATION. The Contractor shall defend, indemnify and hold harmless WSCA-NASPO, the Lead State and Participating Entities along with their officers, agencies, and employees as well as any person or entity for which they may be liable from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement. This section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

12. INDEMNIFICATION – INTELLECTUAL PROPERTY. The Contractor shall defend, indemnify and hold harmless WSCA-NASPO, the Lead State and Participating Entities along with their officers, agencies, and

employees as well as any person or entity for which they may be liable ("Indemnified Party") from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim"). The Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless:
(1) the Product, system or method is:
(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;
(b) specified by the Contractor to work with the Product; or
(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or
(2) it would be reasonably expected to use the Product in combination with such product, system or method.
The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. This section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

13. INDEPENDENT CONTRACTOR. The contractor shall be an independent contractor, and as such shall have no authorization, express or implied to bind WSCA-NASPO or the respective states to any agreements, settlements, liability or understanding whatsoever, and agrees not to perform any acts as agent for WSCA-NASPO or the states, except as expressly set forth herein.

14. INDIVIDUAL CUSTOMER. Except to the extent modified by a Participating Addendum, each Participating Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or to recover any costs allowed in the Master Agreement and applicable Participating Addendum for their purchases. Each Participating Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Participating Entity individually.

15. INSURANCE. Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in the Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or at a Participating Entity's option, result in termination of its Participating Addendum.

Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

a) Commercial General Liability covering the risks of bodily injury (including death), property damage and personal injury, including coverage for contractual liability, with a limit of not less than $1 million per occurrence/$2 million general aggregate;
b) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Participating Entity by the Contractor.

Prior to commencement of the work, Contractor shall provide to the Participating Entity a written endorsement to the Contractor's general liability insurance policy that (i) names the Participating Entity as an additional insured, (ii) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating Entity has been given at least thirty (30) days prior written notice, and (iii) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of the Participating Entity as secondary and noncontributory.

Contractor shall furnish to Participating Entity copies of certificates of all required insurance within thirty (30) calendar days of the Participating Addendum's effective date and prior to performing any work. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at State's sole option, result in this Master Agreement's termination.

Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement.

16. LAWS AND REGULATIONS. Any and all supplies, services and equipment offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

17. LICENSE OF PRE-EXISTING INTELLECTUAL PROPERTY. Contractor grants to the Participating Entity a nonexclusive, perpetual, royalty-free, irrevocable, unlimited license to publish, translate, reproduce, modify, deliver, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The license shall be subject to any third party rights in the Pre-existing Intellectual Property. Contractor shall obtain, at its own expense, on behalf of the Participating Entity, written consent of the owner for the licensed Pre-existing Intellectual Property.

18. NO WAIVER OF SOVEREIGN IMMUNITY. In no event shall this Master Agreement, any Participating Addendum or any contract or any purchase order issued thereunder, or any act of a Lead State or a Participating Entity, be a waiver by the Participating Entity of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

If a claim must be brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for the Participating State. This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. ORDER NUMBERS. Contract order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

20. PARTICIPANTS. WSCA-NASPO is the cooperative purchasing arm of the National Association of State Procurement Officials. It is a cooperative group contracting consortium for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.,) for all states and the District of Columbia. Obligations under this contract are limited to those Participating States who have signed a Participating Addendum where contemplated by the solicitation. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions. Unless otherwise specified in the solicitation, the resulting award(s) will be permissive.

21. ENTITY PARTICIPATION. Use of specific WSCA-NASPO cooperative contracts by state agencies, political subdivisions and other entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

22. PAYMENT. Payment for completion of a contract is normally made within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

23. PUBLIC INFORMATION. This Master Agreement and all related documents are subject to disclosure pursuant to the Participating Entity's public information laws.

24. RECORDS ADMINISTRATION AND AUDIT. The contractor will maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the contractor for costs authorized by this contract. These records will be retained by the contractor for at least four years after the contract terminates, or until all audits initiated within the four years have been completed, whichever is later. The contractor agrees to allow WSCA-NASPO, State and Federal auditors, and state agency staff access to all the records of this Master Agreement and any order placed under this Master Agreement, for audit and inspection, and monitoring of services. Such access will be during normal business hours, or by appointment.

25. REPORTS. The contractor shall submit quarterly reports to the WSCA-NASPO Contract Administrator showing the quantities and dollar volume of purchases by each participating entity.

26. STANDARD OF PERFORMANCE AND ACCEPTANCE. The Standard of Performance applies to all Product(s) purchased under this Master Agreement, including any additional, replacement, or substitute Product(s) and any Product(s) which are modified by or with the written approval of Contractor after Acceptance by the Participating Entity. The Acceptance Testing period shall be thirty (30) calendar days or other time period identified in the solicitation or the Participating Addendum, starting from the day after the Product is installed and Contractor certifies that the Product is ready for Acceptance Testing. If the Product does not meet the Standard of Performance during the initial period of Acceptance Testing, Participating Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the Standard of Performance is met. Upon rejection, the Contractor will have fifteen (15) calendar days to cure the Standard of Performance issue(s). If after the cure period, the Product still has not met the Standard of Performance Participating Entity may, at its option: (1) declare Contractor to be in breach and terminate the Order; (2) demand replacement Product from Contractor at no additional cost to Participating Entity; or, (3) continue the cure period for an additional time period agreed upon by the Participating Entity and the Contractor. Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section. No Product shall be accepted

and no charges shall be paid until the Standard of Performance is met. The warranty period will begin upon Acceptance.

27. SYSTEM FAILURE OR DAMAGE. In the event of system failure or damage caused by the Contractor or its Product, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

28. TITLE OF PRODUCT. Upon Acceptance by the Participating Entity, Contractor shall convey to Participating Entity title to the Product free and clear of all liens, encumbrances, or other security interests. Transfer of title to the Product shall include an irrevocable and perpetual license to use the Embedded Software in the Product. If Participating Entity subsequently transfers title of the Product to another entity, Participating Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license shall be at no additional cost or charge to either Participating Entity or Participating Entity's transferee.

29. WAIVER OF BREACH. Failure of Lead State or Participating Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State or Participating Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or breach of any terms or requirements shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement or Participating Addendum.

30. WARRANTY. The Contractor warrants for a period of one year from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the solicitation or for which the Participating Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects. Upon breach of the warranty, the Contractor will repair or replace (at no charge to the Participating Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

31. ASSIGNMENT OF ANTITRUST RIGHTS. Contractor irrevocably assigns to a Participating Entity any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

Contractor shall require any subcontractors hired to perform any of Contractor's obligations, under this Master Agreement or Participating Addendum, to irrevocably assign to a Participating Entity, as third party beneficiary, any right, title or interest that has accrued or which may accrue in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the subcontractor for the purpose of carrying out the subcontractor's obligations to the Contractor in pursuance of

this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

32. WSCA-NASPO eMARKET CENTER. Awarded responders are required to participate in the WSCA-NASPO eMarket Center and, working through WSCA-NASPO's contractor (SciQuest), connect with the eMarket Center. The ideal situation would be to use either a hosted (by SciQuest) or Punchout Level 2 catalog configurations, but actual requirements will be determined by the Lead State Contract Administrator, WSCA-NASPO, WSCA-NASPO's contractor (SciQuest) and the awarded contractor, after award. Participation does not require an awarded responder to have any special level of technology or technological understanding.

Definitions:

Acceptance - means a written notice from a purchasing entity to contractor advising Contractor that the Product has passed its Acceptance Testing. Acceptance of a product for which acceptance testing is not required shall occur following the completion of delivery, installation, if required, and a reasonable time for inspection of the product, unless the Purchasing Entity provides a written notice of rejection to contractor.

Acceptance Testing - means the process for ascertaining that the Product meets the standards set forth in the section titled Standard of Performance and Acceptance, prior to Acceptance by the Purchasing Entity.

Contractor - means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

Intellectual Property – means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State - means the State conducting this cooperative solicitation and centrally administering any resulting Master Agreement with the permission of the Signatory States.

Master Agreement – means the underlying agreement executed by and between the Lead State, as WSCA-NASPO contract manager, acting on behalf of WSCA-NASPO, and the Contractor, as now or hereafter amended.

Order - means any purchase order, sales order, or other document used by a Participating Entity to order the Products.

Participating Addendum - means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements ,e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity - means a state, or other legal entity, properly authorized by a state to enter into the Master Agreement or Participating Addendum or who is authorized to order under the Master Agreement or Participating Addendum.

Product - Any equipment, software (including embedded software), documentation, or deliverable supplied or created by the Contractor pursuant to this Master Agreement.

WSCA-NASPO - is a cooperative group contracting consortium for state procurement officials, representing departments, institutions, agencies, and political subdivisions (i.e., colleges, school districts, counties, cities, etc.) for all states and the District of Columbia. WSCA-NASPO is a cooperative purchasing arm of the National Association of State Procurement Officials (NASPO).

APPENDIX C CONTRACTOR INFORMATION AND PROFILE

1. **Company Name**: Sentinel Offender Services, LLC
   Address: 201 Technology Drive
   City: Irvin State: California Zip: 92618
   Phone: (888) 843-5590 FAX: (800) 327-1178
   Washington State Department of Revenue Registration Tax number: 602570600
   Federal Tax ID No.: 33-0929945
   Company Internet URL Address: www.sentrak.com

2. **Legal Status of the Bidder:** Limited Liability Company (LLC)

3. **Bidder's Authorized Representative: (**Reference Section 2.3)
   Name: Leo Carson, Vice President of Strategic Sales
   Phone: (888) 843-5590 FAX: (800) 327-1178 E-mail: leo.carson@sentrak.com

4. **Orders to be sent to; Billing will be from; and Payment to be sent to:**
   Company Name: Sentinel Offender Services, LLC
   Address: 201 Technology Drive
   City: Irvin State: California Zip: 92618
   Phone: (888) 843-5590 FAX: (800) 327-1178 E-mail: leo.carson@sentrak.com
   Internet address for company catalog: www.sentrak.com

5. **Contact Person for Sales Reports to be filed with MCC: (**Reference Section 2.10)
   Contact Person's Name: Leo Carson, Vice President of Strategic Sales
   Phone: (888) 843-5590 FAX: (800) 327-1178 E-mail: leo.carson@sentrak.com

6. **Bidder's Company Experience and History:** Upon request, Contractor will provide information about the company's experience and history in providing electronic monitoring of offenders equipment and services.

7. **Minority/Women Owned Business (MWBE):** No: X

8. **Payment Methods and Terms:**
   Payment Terms: Net 30 days. Purchasing (charge) Cards (credit and/or debit cards) accepted include: Visa, Mastercard and Discover. No additional card fee or processing charge shall be permitted.

9. **Purchasing Cooperative Members – Washington State Political Subdivision and Nonprofit Corporations:** Contractor agrees to sell the goods and services on this contract to political subdivisions and nonprofit corporations which are members of the State of Washington Purchasing Cooperative (WSPC): Yes X.

10. **Subcontractors:** Contractor may obtain alcohol devices from subcontractors in the performance of this contract.

11. **Customer References:** Customers may contact the Contractor for a list of references for any category of electronic monitoring of offenders equipment and service available through this Contract.

APPENDIX D SPECIFICATIONS

SPECIFICATIONS

These specifications are the minimum. The vendor has listed, clearly demonstrated, and presented features that add value, savings and/or reliability.

CATEGORY 1 – RADIO FREQUENCY (RF) CONTINUOUS SIGNALING ELECTRONIC MONITORING SERVICE			
1.0	**SECTION A Vendor Requirements**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
1.1	Vendor Requirements	The Vendor must have at least two (2) years of experience delivering Radio Frequency monitoring services.	**Sentinel exceeds this requirement. Sentinel has been providing electronic monitoring and participant supervision including radio frequency monitoring services for more than 20 years since its founding in 1992 and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Radio Frequency electronic monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel is still currently in the business of providing electronic monitoring services to community corrections and/or criminal justice organizations and since its inception has had more than 1,000,000 participants successfully completed their programs through Sentinel's extensive continuum of community-based monitoring services. **Sentinel is proposing its latest generation, most advanced radio frequency monitoring solution, RF Patrol®, which has been in use for more than five (5) years in agencies nationwide, including but not limited to WSCA customers. All of Sentinel's services, products and technologies are specifically designed for corrections supervision and will meet or exceed the requirements for the Electronic Monitoring of Offender through the Western States Contracting Alliance.** Please see the Bidder's Company Experience and History section of this proposal for more detailed information on Sentinel's experience in the provision of radio frequency monitoring services.

1.2	Vendor Requirements	Vendor must be capable of performing expert On-Site Service and be capable of dispatching expert technicians to the field in the event electronic diagnosis or replacement of component problems are encountered.	**Sentinel exceeds this requirement.** Sentinel is capable of performing expert onsite service and capable of dispatching expert technicians to the field in the event electronic diagnosis or replacement of component problems are encountered. Sentinel's extensive depth of field services personnel (See the following organizational chart) will provide corporate oversight for the contractual cycle of each of the participating programs during the program lifecycle. **The assigned field services personnel will be dispatched to provide on-site service in the event of the need for electronic diagnosis or replacement of component problems.** Field services personnel will also be responsible for scheduling training, per the contract, with agency staff on the use of equipment and reading reports. **Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Radio Frequency electronic monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel has a proven track record of providing excellent performance and flexibility to its customers and commits this to continue this same ongoing dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all services including but not limited to technical assistance, customer support, inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value. **IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.**

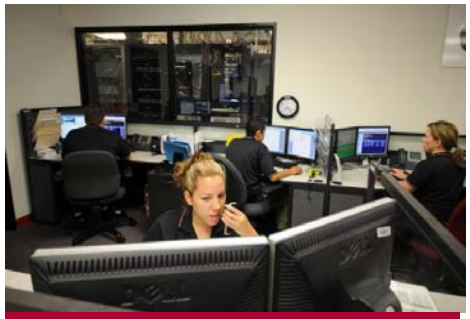
This strong nation-wide presence of qualified Sentinel staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract.

Additionally, staffed monitoring services and technical support are available from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.**

Please see the Bidder's Company Experience and History section of this proposal for more detailed information on Sentinel's proposed field services including biographical sketches of each of the proposed personnel.

1.3	Vendor Requirements	The proposed monitoring device must have been installed and in use on at least an aggregate of 500 offenders through one or more contracts with State, Federal or local government agencies. This experience must include at least six (6) months of active monitoring for the model offered in response to this RFP. The Vendor's experience shall have been met with the vendor acting as the prime contractor in providing all of the above service. Identify these agencies, volumes and devices in your proposal response.	**Sentinel exceeds this requirement.** Sentinel is proposing its latest generation, most advanced radio frequency monitoring solution, RF Patrol®, which has been in use for more than five (5) years in agencies nationwide and has been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Furthermore, RF Patrol® is the RF system for the incumbent WSCA contract. Sentinel has provided a list containing the State, Federal or local government agencies exceeding the minimum specified the volumes for RF Patrol® monitoring equipment in the Appendix D: Bidder Information and Profile section of this proposal as required. **Sentinel has been providing electronic monitoring and participant supervision including radio frequency monitoring services for more than 20 years since its founding in 1992 and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Radio Frequency electronic monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel is still currently in the business of providing electronic monitoring services to community corrections and/or criminal justice organizations and since its inception has had more than 1,000,000 participants successfully completed their programs through Sentinel's extensive continuum of community-based monitoring services.
1.4	Vendor Requirements	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.	**Sentinel exceeds this requirement. Sentinel was the first to develop and is the most experienced company providing Internet information exchange for monitoring and tracking information.** Sentinel's legacy Internet information exchange platform, **WEB PATROL®**, has been in successful operation with customers over the past nine (9) years. **SenTrak, Sentinel's advanced Internet information exchange platform, functions fully with Sentinel's RF Patrol® monitoring equipment and has been in use consecutively for more than five (5) years in support of State, Federal and local government agencies, including but not limited to incumbent WSCA customers.** Sentinel is prepared to continue providing the WSCA participating agencies its latest generation **RF PATROL®** conventional active radio frequency electronic monitoring units supported by Sentinel's web-based Internet information exchange, **SenTrak**, designed to allow agency personnel to manage an offender's data and schedule through the use of a standard web browser.

1.5	Vendor Requirements	All devices shall be currently registered and approved by the Federal Communications Commissioner (FCC).	**Sentinel meets this requirement.** All devices are currently registered and approved by the Federal Communications Commissioner (FCC). Sentinel has provided the Identifier Numbers below and copies of the certifications are included in the Exhibits section of this proposal: **Part 15** ▪ RF Patrol® PTX NSNPTX08 ▪ RF Patrol® PHMU Landline NSNPHMUL08 ▪ RF Patrol® PHMU Cellular NSNPHMUC08 ▪ RF Patrol® OPID NSNOPID08 ▪ RF Patrol® Drive-By NSNPMD09 **Part 68** ▪ RF Patrol® US:YEVMM06BPHMUL08
2.0	**SECTION B Monitoring Center Facility, Data Center. Data Storage and Data Access**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
2.1	Facility	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 Government agencies at the time of proposal submittal. This experience shall be with the same government agencies listed in Item 1.3. The Vendor shall have been the prime contractor for any contract services performed by any subcontracted monitoring service center or help-desk facility.	**Sentinel exceeds this requirement. As the incumbent provider of the WSCA's radio frequency monitoring program since January 2, 2002 (more than 11 years), Sentinel has proven experience and capability to provide the required radio frequency electronic monitoring equipment to all participating agency offenders.** The Sentinel monitoring center facility and services have been in use for at least six (6) consecutive months through one or more contracts with State Government agencies at the time of proposal submittal (many of these agencies have contracted with Sentinel for 10 years or more). This experience has been with the same government agencies listed in the Appendix D: Bidder Information and Profile section of this proposal as required. Sentinel is the prime contractor for any contract services performed – All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. Sentinel **owns and operates** both its primary monitoring center located in Irvine, California **that has been in operation in excess of six (6) consecutive months,** and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the- art facility, located in Irvine, California that is staffed 24 hours a

			day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis. The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted and information is disseminated. It is complete with men's/women's restrooms, vending machines, and emergency equipment all designed to ensure uninterrupted performance and create a comfortable staff environment. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center.  Customer service through Sentinel's 24 hour a day monitoring center All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a monitoring center failure or service catastrophe.**
2.2	Facility	The Vendor shall provide a secure confidential monitoring service center and help-desk facility that provides service 24/7/365.	**Sentinel meets this requirement. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis providing secure confidential monitoring services.** The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted, monitoring information is disseminated and technical support (help desk) services are provided.

			Sentinel owns and operates both its primary monitoring center located in California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. To maintain monitoring center operational integrity and confidentially, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.

			IMPORTANT SENTINEL ADVANTAGE: The Sentinel monitoring center has been servicing WSCA participating agencies since January 2, 2002 (over 11 years). Sentinel understands the objectives of the Western States Contracting Alliance program better than any other vendor in the industry. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** The Western States Contracting Alliance participating agencies can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year. Sentinel strives to resolve any customer inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns.

			Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards. The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **IMPORTANT SENTINEL ADVANTAGE: The Sentinel monitoring center has been servicing WSCA participating agencies since January 2, 2002 (over 11 years). Sentinel understands the objectives of the Western States Contracting Alliance program better than any other vendor in the industry.** **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** The Western States Contracting Alliance participating agencies can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.

			Sentinel strives to resolve any customer inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Regional Account Manager/Field Operations Manager for customer enhancement requests, suggestions and ideas.
2.3	Facility	Monitoring Center will be clean, well-maintained, safe and secure for personnel as well as compliant with all Federal Regulations regarding safety.	**Sentinel meets this requirement. The continuously staffed Sentinel monitoring center resides in an independently secured, safe, climatecontrolled facility with raised floors, a fire suppression system and written policies and procedures for access that meet all applicable federal, state and local regulations regarding safety**. The primary monitoring center is a separate, self-supporting node within the Irvine facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. **It is clean and well-maintained** complete with men's/women's restrooms, vending machines, and emergency equipment all designed to ensure uninterrupted performance and create a comfortable staff environment.

2.4	Facility	Monitoring Center must be secure from unauthorized entry or malicious actions against facility and staff.	**Sentinel meets this requirement. The Sentinel monitoring center is secure from unauthorized entry or malicious actions against facility and staff. Physical Security of Facilities:** The continuously staffed Sentinel monitoring centers reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: Enforces an electronic key card system for entryway access to both outside building and monitoring center Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center.

			As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified.
2.5	Facility	Monitoring Center must have disaster mitigation features (e.g. fire resistant, earthquake resistant; hurricane resistant.)	**Sentinel meets this requirement. The Sentinel monitoring center has multiple disaster mitigation features, resides in an independently secured, climate-controlled facility with raised floors, a fire suppression system** and written policies and procedures for access. The Sentinel monitoring center meets **all applicable federal, state and local regulations regarding safety including building codes regarding earthquake resistance and hurricane resistance.** **Power Redundancy:** Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-theart technology including: ▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator.

			Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's onsite diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled. The diesel generator is regularly inspected to ensure that it remains in operational order at all times. **Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days (in excess of 72 hours). Sentinel has never lost any data or performance capability due to power losses of any sort.** **Communications Redundancy:** The Sentinel monitoring center features the following technology for its Internet and telephone communications: ▪ T-1 telephone trunks, provided from three (3) redundant leading providers, to prevent against outages ▪ 432 Fiber-optic telecom cable lines and 200 POTS lines fed directly into the Sentinel facility ▪ Primary provider, Cox Communications (a leading provider of communications) is regionally headquartered within 8 miles and has triple electrical and data redundancy ▪ Second redundant carrier, AT&T ▪ Third redundant carrier, TW Telecom ▪ Cisco IP Telephony Solution combined with Cisco Networking for providing statistical tracking of all data and telephone activity A confidential, predefined and rehearsed protocol is set up with Sentinel's telecoms provider to enable a rapid transfer in accordance with the agreed service level. The back-up call handler functions in an active state and is ready to receive calls from the monitoring units as soon as the calls are rerouted from the primary call handler by Sentinel's Telecom providers.

			Redundant Monitoring Center: To support business operations for database replication of key IT, electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a redundant monitoring center. While Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart. Sentinel offers full on-site and full off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. **Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster.** Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.6	Facility	In the event of a disaster the Vendor must have a backup Monitoring Center 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.	**Sentinel meets this requirement.** Sentinel operates two (2) geographically redundant monitoring centers in Irvine, California and Atlanta, Georgia. To support business operations for electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a fully-redundant monitoring center. Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia more than 500 miles apart 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. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, Sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day. Sentinel's primary**

			Irvine, California monitoring center is staffed 24 hours a day, seven (7) days a week, 365 days a year. Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center. Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.7	Facility	Deleted	
2.8	Facility	The exchange of monitoring information (including enrollment, data changes, monitoring reports and terminations) between Officers and the Vendor's Monitoring Center facility shall occur via secure, real-time access to Vendor's web-based system by Officer's using existing agency computers/Internet access.	**Sentinel meets this requirement.** The exchange of monitoring information (including enrollment, data changes, monitoring reports and terminations) between officers and Sentinel's monitoring center facility occur via secure, realtime access to Sentinel's web-based information system by officer's using existing agency computers/Internet access. Sentinel's equipment offerings discussed in this proposal are designed specifically for continuous and real-time electronic monitoring and supported by Sentinel's two (2) redundant monitoring centers through multiple communication methods including toll-free telephone, email, fax and the proposed web-based software platform. The computer systems, through SenTrak, immediately and automatically (in real-time) store all of the data entered at the time of enrollment, data and/or monitoring changes, monitoring reports and terminations exchanged between officers and the monitoring center facility. SenTrak allows all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) to exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access. SenTrak date and time stamps,

			monitoring center using secure website access. SenTrak date and time stamps, and records the user login name for all remote data entries. Users have the ability to directly access participant information through Sentinel's SenTrak. The SenTrak system provides users with real-time access to participant events, daily statuses and caseload data.
2.9	Facility	The Vendor shall have written operational and procedure manuals and disaster recovery plans for the Monitoring Center(s) (all locations). All revisions/updates by the Vendor to such manuals shall be forwarded to the Agency as they occur. The Agency will review such manuals and plans to ensure the integrity of the electronic monitoring system is maintained. While it is not necessary for the vendor to submit these documents with proposal, they must be provided to any requesting agency post award.	**Sentinel meets this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing both monitoring centers and the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel customizes its Risk Mitigation and Disaster Recovery Plan to each agency upon contract award. Sentinel considers this mission critical plan highly confidential yet, will provide copies of to authorized individuals at any requesting agency post award. All revisions/updates to this plan will be forwarded to the agency as they occur. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel is ISO 9001:2008 certified and maintains ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations including agency/departmental specific operational procedures for disaster recovery, technical support and customer service. Sentinel operates two (2) geographically redundant monitoring centers in Irvine, California and Atlanta, Georgia. Redundant web servers, application servers and database servers, are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery.
2.10	Facility	The system will synchronize with daylight savings time.	**Sentinel meets this requirement.** Sentinel's proposed systems **synchronize with daylight savings time.** The proposed web-based monitoring platform, SenTrak uses Coordinated Universal Time (UTC) so therefore there is no daylight savings time adjustment necessary in the code. However, all of the time stamps for incoming reports from the RF Patrol® PHMUs use the server's time for storage and notifications to customers. Sentinel synchronizes all server times to daylight savings time through the following methods: ▪ Windows 2003/2008 servers are configured to automatically adjust for DST in the server's time settings ▪ Sentinel manages the clock synchronization for all of its servers with a product called Domain Time II. This software synchronizes the domain controller with an external public NTP server to ensure the clock is accurate. It then installs an agent on all other servers that constantly monitors the clocks to ensure they are accurate within a few milliseconds of the main domain controller server. This corrects any

			▪ potential clock drift from server to server which can result in incorrect time stamps on incoming reports from the PHMU.
2.11	Facility	The Vendor's Monitoring Center should have a permanently installed and functioning emergency backup power source, independent of its main power source, capable of maintaining continuous operation until primary power is restored or the backup Monitoring Center is fully functional.	**Sentinel exceeds this requirement. Sentinel's monitoring center have permanently installed and functioning emergency backup power sources, independent of its main power source, capable of maintaining continuous operation until primary power is restored or the backup monitoring center is fully functional.** Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week. Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster. Sentinel monitoring center is outfitted with the latest state-of-the-art technology including: ▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator.
			Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's onsite diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. **Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled.** The diesel generator is regularly inspected to ensure that it remains in operational order at all times. Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days. Sentinel will institute fail-over procedures to the back-up monitoring center should any continuous commercial power outage

			back-up monitoring center should any continuous commercial power outage occur that jeopardizes monitoring center operations. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.12	Facility	The Vendor's Monitoring Center should have ventilation and temperature controls adequate to ensure proper functions of the Monitoring Center hardware.	**Sentinel meets this requirement. The continuously staffed Sentinel monitoring center resides in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community.**
2.13	Facility	The Vendor's Monitoring Center's physical security features at a minimum should include closed circuit camera system and limited access doorways. Describe other features to ensure physical security.	**Sentinel exceeds this requirement.** To maintain monitoring center operational integrity, and physical security, Sentinel's monitoring center's physical security features include closed circuit camera system and limited access doorways. Additionally, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure

			username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labeled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified.
2.14	Data Center	The facility housing the Data Center(s) must have multiple physical security features. Describe the physical security features that protect the Data Center and agency data.	**Sentinel meets this requirement.** The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the data centers utilized to support the **RF Patrol**® monitoring solution. Additionally, this is the central location from which all monitoring center activities are conducted and information is disseminated. **Physical Security of Facilities:** The continuously staffed Sentinel monitoring centers reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that

			meet all applicable federal, state and local regulations and do not endanger the operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building.

			The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified. **Security of Monitoring Records:** In Sentinel's experience with offender populations nationwide, Sentinel understands the importance of data integrity both in its actual data entry as well as its subsequent data retention. To ensure that the proper information is entered at all times, Sentinel's personnel are thoroughly trained on data entry procedures with supervisorial support for any adjustments or corrections. Each user is given their own login and once they set their confidential password Sentinel can ensure the integrity of each user's entry. This unique user access allows Sentinel's Information Technology personnel to follow electronic audit trails that allow supervisors and management to verify the source of all date entry. All data is actually stored on Sentinel's central servers located in its secure corporate facility. The workstations that Sentinel's staff and Agency personnel use at local facilities are technically only used to connect to Sentinel's central server. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. In addition, Sentinel's monitoring center and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure, the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery Procedures and restart systems according to procedure. Sentinel's Engineering

			Procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Any instance of failure resulting in a loss of monitoring capability will be reported to the participating agency. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. All of Sentinel's security systems are monitored continuously. **Monitoring System Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. To prevent unauthorized access from outside the monitoring center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platform and case management software use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made. Sentinel's monitoring system is only accessible via a Cisco ASA firewall blocking any unauthorized access form the Internet to ensure the remote connection is not compromised. **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI

			Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
2.15	Data Center	The Vendor's Data Centers must have ventilation and temperature control adequate to ensure proper functions of the Data Center hardware.	**Sentinel meets this requirement.** Sentinel's data centers have ventilation and temperature control adequate to ensure proper functions of the system hardware. The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the data centers utilized to support the **RF Patrol**® monitoring solution. Additionally, this is the central location from which all monitoring center activities are conducted and information is disseminated. The continuously staffed Sentinel monitoring center resides in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community.
2.16	Data Center	The Vendor's Data Centers must have back-up emergency power generators.	**Sentinel exceeds this requirement.** The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the primary data centers utilized to support the **RF Patrol**® monitoring solution. Additionally, this is the central location from which all monitoring center activities are conducted and information is disseminated. Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100%

			at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-the-art technology including but not limited to back-up emergency power generators: - Fault tolerant central computer system offering maximized uptime. - APC Symetra battery back-up Uninterruptible Power Supply (UPS). - Kohler 150kVA diesel generator. Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's onsite diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. **Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled.** The diesel generator is regularly inspected to ensure that it remains in operational order at all times. Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days. Sentinel will institute fail-over procedures should any continuous commercial power outages occur that jeopardizes participant monitoring. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers are located in Atlanta, Georgia, over 500 miles apart. To support operations for database replication of key IT and failover disaster recovery, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers at a state-of-the-art, fully-secured facility that has both redundant short-term and long-term power

			supplies. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full on-site and full off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. **Sentinel has never lost any data or performance capability due to power losses of any sort.**
2.17	Data Center	The Vendor must have redundant Data Centers 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 Data Center.	**Sentinel exceeds this requirement.** Sentinel has a redundant monitoring center located sufficiently distant from the primary center, that 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. To support business operations for database replication of key IT, and failover disaster recovery, Sentinel's monitoring system incorporates redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and redundant DRP servers are located in Atlanta, Georgia, **over 500 miles apart**. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full on-site and full offsite redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a manmade or natural event the causes major disruption to electrical or communications services to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred.

			Additionally, access to Sentinel's web-based information exchange platform is automatically redirected to the back-up web server if the primary monitoring center fails. Sentinel's web-based information exchange platform uses a **Uniform Resource Locator (URL)** that is defined with both primary and back-up servers to automatically and transparently redirect users in case of failover.
2.18	Data Center	All back-up systems in the Data Centers must be tested regularly.	**Sentinel exceeds this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing both monitoring centers and the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel customizes its Risk Mitigation and Disaster Recovery Plan to each agency upon contract award and will provide this plan to any requesting agency post award. All revisions/updates to this plan will be forwarded to the agency as they occur. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. **Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.** **IMPORTANT SENTINEL ADVANTAGE:** A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure, the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. All of Sentinel's security systems are monitored continuously.

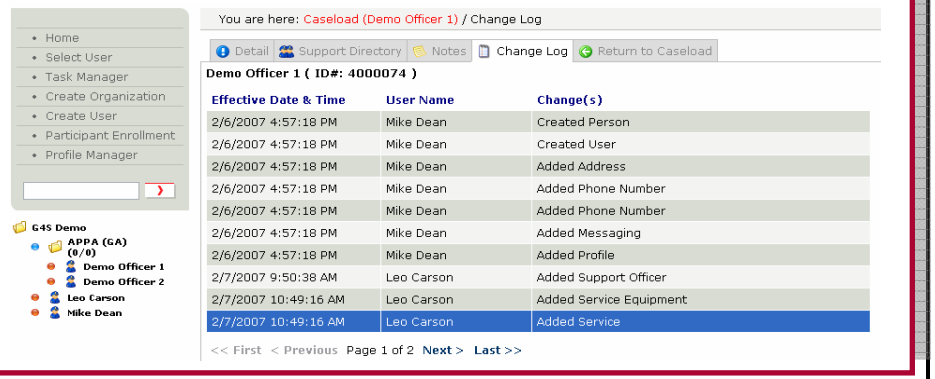
2.19	Data Center	The Vendor's system should provide for 100% redundancy to avoid unnecessarily excessive downtime due to hardware or software issues. In the event of data disruption, the secondary Data Center must be activated within 60 minutes of initial system failure.	**Sentinel exceeds this requirement.** Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that serves to immediately protect all computers and electronic equipment from downtime continuing to power the entire monitoring center as normal and can do so while Sentinel's on site diesel generator automatically begins operation. To support operations for database replication of key IT, and failover disaster recovery to avoid unnecessarily excessive downtime due to hardware or software issues, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers are located in Atlanta, Georgia, over 500 miles apart. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. Redundant web servers, application servers and database servers, are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be **no interruption in participant monitoring** and no data lost from the monitoring units because data is stored until it is successfully transferred. Sentinel uses an industry standard data protection and recovery software package to ensure that the databases within the primary and back-up data servers are concurrently maintained, which ensures the following: ▪ No loss of data from the databases if there is a failover ▪ Capability for the back-up database to immediately and automatically become available for processing and access The system maintains a constant connection between the primary and back-up database servers and when it detects the loss of a regular "heartbeat" signal between the systems, it automatically initiates an alert notifying Sentinel of this loss. It is then determined if the loss of heartbeat was an anomaly or it is warrants a real-time failover from the primary database server to the back-up server. Regardless of the cause, **Sentinel's contingency plans will failover in**

			the case of any system malfunction that effects participant monitoring or reporting, which cannot be corrected within one (1) hour. Additionally, access to Sentinel's web-based information exchange platform, SenTrak, is automatically redirected to the back-up web server if the primary monitoring center fails. Sentinel's web-based information exchange platform uses a **Uniform Resource Locator (URL)** that is defined with both primary and back-up servers to automatically and transparently redirect users in case of failover. Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.20	Data Storage	The Vendor must ensure that all records (automated or hard copy files) remain the property of the Agency and shall be returned within 30 days, in the event the contract is canceled or terminated.	**Sentinel meets this requirement.** All records created for participants referred to this program by any participating agency will remain solely the property of the participating agency. Upon completion of services, all records will be returned to the participating agency within 30 days or destroyed under direction of agency staff.
2.21	Data Storage	The Vendor's system must ensure that all data be recorded with a historical transaction record and stored/archived for retrieval/backup in a database when requested by Agency personnel in accordance with the following:	**Sentinel meets this requirement.** The computer system, through SenTrak, immediately and automatically (in real-time) records with a historical transaction record all of the data received by the monitoring equipment, entered at the time of enrollment, data and/or monitoring changes, monitoring reports and terminations exchanged between officers and the monitoring center facility. And stores/archives for retrieval/backup. SenTrak and stores/archives for retrieval/backup all monitoring data so that all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) can view or exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access.

2.22	Data Storage	a. All historical data must be centrally stored and accessible for reporting purposes;	**Sentinel meets this requirement.** SenTrak and stores/archives for retrieval/backup all monitoring data so that all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) can view or exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access.
2.23	Data Storage	b. This information must be available for reporting in a standard transaction file format; and	**Sentinel exceeds this requirement.** Authorized users have the ability to directly access all participant historical information through Sentinel's SenTrak. The SenTrak system also provides users with real-time and historical access to participant events, daily statuses and caseload data for reporting purposes. All monitoring reports are available through the easy-to-use report generator application of Sentinel's SenTrak software. Participant activity is posted in realtime so users can view violations online as they occur or a record of any historical data. Any authorized user can view participant activity 24 hours a day, seven (7) days a week, 365 days a year. Sentinel will work with its clients to ensure all needed reports, including on-demand, daily and quarterly reports are available. **All reports in SenTrak can be viewed on screen, printed or exported in XML, CSV, TIFF, PDF, HTTP or Excel formats.**
2.24	Data Storage	c. All current and historical data files must be retained for a minimum of seven (7) years and this information shall be available at no charge to the Agency.	**Sentinel exceeds this requirement.** Sentinel secures all system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. Databases are backed up on removable discs, using the industry recognized Symantec Backup Exec software data backup and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel.

			If system recovery is necessary, Sentinel is not limited to the sole use of back-ups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler. Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups.
2.25	Data Storage	The Vendor's Data Centers must have duplicate computers with the ability to, at a minimum, permit restoration of data collection and user monitoring services within ten (10) minutes after computer failure. The Monitoring Center should have duplicate data storage devices with automated fail-over and automatic re-establishment of the duplicate databases upon replacement of the failed storage device.	**Sentinel exceeds this requirement.** The Sentinel's monitoring centers have duplicate computers with the ability to continue data collection and user monitoring services uninterrupted in the event of a computer failure. The monitoring center has duplicate data storage devices with automated fail-over and automatic reestablishment of the duplicate databases upon replacement of any failed storage device.The workstations within Sentinel's monitoring centers are equipped with redundant features; all of the computer systems in Sentinel's monitoring centers are designed to perform the same monitoring functions. They are all "ghosted" or duplicate workstations that process the incoming signals similarly. If one of the computers is not functioning properly, all incoming signals are simply routed **immediately** to one of the other available computers. In addition, Sentinel employs internal Information Technology personnel based here at the same facility. In the event that a computer, facsimile or modem error occurs, Sentinel's IT personnel quickly replace the computer component with no affect on the alarm processing capabilities of the entire system. Along with spare computer workstations, Sentinel has additional equipment available to replace facsimile machines, modems and all other monitoring center components thus allowing seamless operation of the Center at all times. Sentinel secures all system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. Databases are backed up on removable discs, using the industry recognized Symantec Backup Exec software data back-up and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure l fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel.

			If system recovery is necessary, Sentinel is not limited to the sole use of backups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler. Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups.
2.26	Data Storage	Upon request from the Agency, 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 the Agency.	**Sentinel meets this requirement.** Upon request, Sentinel will provide the most up-to-date complete copy of the respective agencies data included in 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 the participating agency.
2.27	Data Access	The Vendor shall 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-Agency personnel, without prior written approval from the Agency Program Manager.	**Sentinel meets this requirement.** At no time will Sentinel ever disclose confidential data including 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 any unauthorized personnel without written approval of the participating agency Program Manager. All program data will be maintained in accordance with secure data protection standards. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.

2.28	Data Access	The Vendor must maintain unaltered recorded data of offender violations, to be accessible in original form and substance for utilization as physical evidence for prosecution.	**Sentinel exceeds this requirement.** The SenTrak system maintains unaltered recorded data of offender violations, accessible in their original form and substance for utilization as physical evidence for prosecution. SenTrak automatically logs all changes performed in SenTrak with the user's name, date and time of the change, and change the user made. Sentinel tracks all changes to the application, including but not limited to participant or agency details, notes, alert resolutions, enrollments, terminations and service requests. This information is viewable through the SenTrak Change Log and provides agencies with a clear audit trail for user accountability. Caseload Status Screen (Change Log Tab) 
2.29	Security	The Vendor shall have written policies and procedures for network security, application security, data transmission and data security, as well as Monitoring Center physical security.	**Sentinel exceeds this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, Monitoring Center physical security as well as its plan to maintain continuous operations in the event of a disaster. Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. **Network Security:** To prevent unauthorized access from outside the monitoring center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platform and case management software use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic**

			information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made. Sentinel's monitoring system is only accessible via a Cisco ASA firewall blocking any unauthorized access form the Internet to ensure the remote connection is not compromised. **Application Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. The password criteria are as follows: ▪ The monitoring system requires a minimum password length of eight (8) characters ▪ Password must meet certain complexity requirements including alphanumeric specifications as well as special characters (Z 1 3 5 7 9 @ # & ! 0 %) ▪ Passwords are required to be changed every 90 days ▪ Password history is infinite so any user accessing the system cannot use any password they have previously used **Data Transmission and Security:** The equipment offerings discussed in this proposal are designed specifically for continuous and real-time electronic monitoring and supported by Sentinel's central computer system located at its secure monitoring center to receive, store, and disseminate data generated through encrypted and secure communication channels. All data is actually stored on Sentinel's central servers located in its secure corporate facility. The workstations that Sentinel's staff and Agency personnel use at local facilities are technically only used to connect to Sentinel's central server. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. In addition, Sentinel's monitoring center and secure web-based monitoring systems incorporate the

			latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **Physical Security:** The continuously staffed Sentinel monitoring centers reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards:

			▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance.

			In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified.
2.30	Security	The system shall provide security features, which prevent unauthorized individuals from accessing any information held by the Vendor. Secure access to the system shall be maintained at all times.	**Sentinel meets this requirement. Monitoring System Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. To prevent unauthorized access from outside the monitoring center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platform and case management software use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** Sentinel's monitoring system is only accessible via a Cisco ASA firewall blocking any unauthorized access form the Internet to ensure the remote connection is not compromised. **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating

			agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
2.31	Security	The Vendor shall maintain security policies and procedures for its network security, application security, data transmission security, data storage security, and physical security. While it is not necessary for the vendor to submit these documents with proposal, they must be provided to any requesting agency post award.	**Sentinel exceeds this requirement.** Sentinel has provided an overview of its security policies and procedures for network security, application security, data transmission security, data storage security and physical security in response to the specification 2.29 in the section of its proposal. Sentinel maintains security policies with its Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, Monitoring Center physical security as well as its plan to maintain continuous operations in the event of power failures, telephone system failures, local equipment failures, flood or fire at the Monitoring Center and/or Data Centers. Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. Post award upon request, Sentinel will supply a requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
2.32	Security	The Vendor shall provide secure transmission and storage of data and shall ensure that all data, data transmissions and data storage is kept confidential.	**Sentinel meets this requirement.** Sentinel provides secure transmission and storage of all monitoring data and has policies and procedures in place to ensure that all data, data transmissions and data storage is kept confidential. **Data Transmission and Security:** The equipment offerings discussed in this proposal are designed specifically for continuous and real-time electronic monitoring and supported by Sentinel's central computer system located at its secure monitoring center to receive, store, and disseminate data generated through encrypted and secure communication channels. All data is actually stored on Sentinel's central servers located in its secure corporate facility. The workstations that Sentinel's staff and Agency personnel use at local facilities are technically only used to connect to Sentinel's central server. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential

			offender data and records will not be compromised. In addition, Sentinel's monitoring center and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. **Application Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. The password criteria are as follows: ▪ The monitoring system requires a minimum password length of eight (8) characters ▪ Password must meet certain complexity requirements including alphanumeric specifications as well as special characters (Z 1 3 5 7 9 @ # & ! 0 %) ▪ Passwords are required to be changed every 90 days ▪ Password history is infinite so any user accessing the system cannot use any password they have previously used **Network Security:** To prevent unauthorized access from outside the monitoring center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platform and case management software use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** Sentinel's monitoring system is only accessible via a Cisco ASA firewall blocking any unauthorized access form the Internet to ensure the remote connection is not compromised.

			Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards. The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
2.33	Security	The Vendor's facility, equipment, data transmissions, and data storage shall be secure. The Vendor's facility shall be alerted and monitored by a local law enforcement agency or security company. The alert line shall be a tamper-resistant dedicated circuit and shall not be exposed to any person or thing that could alter or damage the line. The Data Center shall be equipped with automated fire detection and suppression equipment.	**Sentinel meets this requirement.** Sentinel has provided an overview of its security policies and procedures for network security, application security, data transmission security, data storage security and physical security in response to the specification 2.29 in the section of its proposal. Sentinel uses multiple security systems including active video/audio systems, alarms system and motion and fire detectors that are monitored by an outside security contractor for supervising the entryways into the facility. The outside security contractor will alert Sentinel each time there is a potential security threat through a tamper resistant dedicated circuit that is secured against any person or thing that could alter or damage the line. The continuously staffed Sentinel monitoring center resides in an independently secured, facility with raised floors, a fire detection and suppression system and written policies and procedures for access that meet all applicable federal, state and local regulations regarding safety.

2.34	Security	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 any requesting agency post award.	**Sentinel meets this requirement.** Sentinel maintains and routinely tests its comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, Monitoring Center physical security as well as its plan to maintain continuous operations in the event of power failures, telephone system failures, local equipment failures, flood or fire at the Monitoring Center and/or Data Centers. Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. Post award and upon request, Sentinel will supply an requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
3.0	**SECTION C Monitoring Center Staff**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
3.1	Monitoring Center Staff	All operators answering calls, monitoring and reporting are required to be certified by Vendor as to full knowledge of systems and ability to operate systems. All Vendors' monitoring staff shall be certified by the Original Equipment Manufacturer and must be well versed in all aspects of the system including but not limited to:	**Sentinel exceeds this requirement. All Sentinel monitoring center operators are certified by the Original Equipment Manufacturer and well versed in all aspects of the system including but not limited to these specified items.** Sentinel **owns and operates** both its primary monitoring center located in Irvine, California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **As such, staffed monitoring services**

			and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. **IMPORTANT SENTINEL ADVANATGE:** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a monitoring center failure or service catastrophe and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Radio Frequency electronic monitoring contractor for more than 11 years since the WSCA contract's inception.** **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's monitoring center is staffed with bilingual personnel on every shift in order to ensure successful interactions with its agency customers. Sentinel monitoring center personnel typically answer 96% of all calls within eight (8) seconds and provide an on-hold wait time of four (4) seconds or less. Additionally, Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including the proposed **RF Patrol®** electronic monitoring solution. All of Sentinel's monitoring center employees undergo a thorough and detailed training and certification program, during which they are trained in all aspects of electronic monitoring equipment and software including troubleshooting and the necessary alarm procedures to ensure timely and accurate notifications. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel monitoring center staff is cross-trained to support assistance requests for radio frequency (RF) electronic monitoring, voice verification monitoring programs breath alcohol testing (BAT), and global positioning satellite (GPS) tracking should any participating agency be utilizing more than one (1) service category. Two (2) full weeks are used during the training of a new monitoring center operator to ensure that a thorough electronic monitoring knowledge based is developed. Complete equipment functionality and software platform protocols must be understood prior to graduation to a Level One Monitoring Center Operator

			The training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge- and performance-based, allowing maximum participation by monitoring center staff and supervisors. The training techniques, tools, and exams are developed by the training coordinator and are required to successfully complete the certification process. The coordinator will conduct training sessions at regularly scheduled intervals; however, each shift supervisor will be instrumental in the development of their employees. **Monitoring Center On-going Training:** To maintain an efficient service oriented organization, Sentinel employs on-going training modules for all positions. This method is applied equally to all monitoring center operators as to allow correct interpretation and dissemination of information to all authorized agency personnel. The training modules for each employee within the monitoring center are delineated. Sentinel is committed to providing the highest level of monitoring services in the industry. A critical element of providing reliable and efficient monitoring is a knowledgeable, professional and well-trained staff. This training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge and performance based, allowing maximum participation by monitoring center staff and supervisors. A grading system has been established to easily identify staff members with certain knowledge and ability. This grading system requires an employee to demonstrate acquired skills through verbal and written examinations. **Levels:** ▪ Monitoring Specialist Level – Trainee ▪ Monitoring Specialist Level – 1 ▪ Monitoring Specialist Level – 2 ▪ Monitoring Specialist Level – 3 ▪ Monitoring Shift Supervisor

Training / Certification: The Training Coordinator is responsible for developing the training techniques, tools, and exams that are required to successfully complete the certification process. The Training Coordinator will conduct training sessions at regularly scheduled intervals; however each shift supervisor will be instrumental in the development of their employees. Training for the various levels will be conducted as follows:

Level	Training Conducted By	Certified By
Trainee	Training Coordinator	Training Coordinator
1	Shift Supervisor	Training Coordinator
2	Shift Supervisor	Training Coordinator
3	Training Coordinator	Training Coordinator
Shift Supervisor	Monitoring Center Manager	Monitoring Center Manager

Certification Exams: A written examination is prepared for each grade level. Some grade levels require that an employee demonstrate acquired skills. A minimum test score is required to pass the written examination.

Level	Minimum Score
Trainee	85%
1	85%
2	85%
3 / Shift Supervisor	90%

A passing score is mandatory for the Trainee and Level 1 position and is required for continued employment. The Level 1 certification exam must be successfully completed before the expiration of a new employee's orientation period. Retesting periods are established to give an employee an additional attempt to achieve a passing score.

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><th>Level</th><th>Testing Period</th><th>Re-Testing Period</th><th>Passing Score</th></tr>
<tr><td>Trainee</td><td>When initial training complete</td><td>14 Days</td><td>Mandatory</td></tr>
<tr><td>1</td><td>10 weeks employment</td><td>14 Days</td><td>Mandatory</td></tr>
<tr><td>2</td><td>90 Days</td><td>30 Days</td><td>Not Mandatory</td></tr>
<tr><td>3</td><td>90 Days</td><td>30 Days</td><td>Not Mandatory</td></tr>
</table>

A passing score is mandatory for continued employment beyond the orientation period for the Trainee and Level 1 grade.

Promotion: This performance-based program ensures that qualified candidates are promoted in a manner consistent with Sentinel’s goal of maintaining a knowledgeable and professional staff. A staff member will be promoted upon successful completion of the certification process. An employee that meets the length of service requirements for a grade promotion must be recommended for advancement by their supervisor. Supervisors are advised to consider the following items before recommending an employee for promotion.

Performance:
▪ Attendance
▪ Dependability
Measuring Tools:
▪ Report
▪ Charts
</td>
</tr>
<tr>
<td>3.2</td>
<td>Monitoring Center Staff</td>
<td>a. Enrolling participants via the Internet for immediate activation of all monitoring services;</td>
<td>Sentinel meets this requirement. All monitoring center operators are require to pass initial training and certification as a Level 1 operator are well versed in all aspects of the RF Patrol® system (equipment and associated software) including but not limited to enrolling participants via the Internet for immediate activation of all monitoring services.</td>
</tr>
<tr>
<td>3.3</td>
<td>Monitoring Center Staff</td>
<td>b. Activating/installing both monitoring and tracking equipment on participants;</td>
<td>Sentinel meets this requirement. All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the RF Patrol® system (equipment and associated software) including but not limited to activating/installing both monitoring and tracking equipment on participants.</td>
</tr>
</table>

3.4	Monitoring Center Staff	c. Accessing, reviewing, and changing participant data via the Internet;	**Sentinel meets this requirement.** All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the **RF Patrol®** system (equipment and associated software) including but not limited to accessing, reviewing, and changing participant data via the Internet.
3.5	Monitoring Center Staff	d. Troubleshooting equipment / monitoring /tracking problems;	**Sentinel meets this requirement.** All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the **RF Patrol®** system (equipment and associated software) including but not limited to troubleshooting equipment / monitoring /tracking problems.
3.6	Monitoring Center Staff	e. Terminating participants via the Internet; and	**Sentinel meets this requirement.** All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the **RF Patrol®** system (equipment and associated software) including but not limited to terminating participants via the Internet.
3.7	Monitoring Center Staff	f. Operators must respond to equipment & system issues, including installation issues.	**Sentinel meets this requirement.** All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the **RF Patrol®** system (equipment and associated software) including but not limited to responding to equipment & system issues, including installation issues.
3.8	Monitoring Center Staff	The Vendor shall ensure their staff is trained and certified to provide technical assistance to Agency staff and deal effectively with all issues regarding the Radio Frequency Electronic Monitoring. When necessary, the Vendor shall develop written operational procedures specific to the Agency's monitoring requirements for reference by their staff.	**Sentinel exceeds this requirement.** Sentinel shall ensures its staff is trained and certified to provide technical assistance to agency staff and deal effectively with all issues regarding Radio Frequency Electronic Monitoring. When necessary, the Sentinel develops written operational procedures specific to the agency's monitoring requirements for reference by Sentinel staff. Sentinel has provided an overview of its Operators Levels training and certification program in response to specification 3.1 of this section. All monitoring center operators are required to pass initial training and certification as a Level 1 operator are well versed in all aspects of the **RF Patrol®** system (equipment and associated software) and therefore able to provide technical assistance to agency staff and deal effectively with all issues regarding the Radio Frequency Electronic Monitoring.

			Sentinel strives to resolve any customer inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and proactively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Regional Account Manager/Field Operations Manager for customer enhancement requests, suggestions and ideas. Sentinel is ISO 9001:2008 certified and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations **including agency/departmental specific operational procedures for monitoring, notification protocols, technical support and/or customer service.**

3.9	Monitoring Center Staff	Vendors shall not employ felons in the performance of this contract. Upon Agency request, Vendor shall 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 any requesting agency post award.	**Sentinel meets this requirement.** Sentinel understands the importance of having qualified, capable, and trustworthy personnel to handle the needs of a program of this complexity where services are provided to an ethnically, racially, chronologically (age), and economically diversified participant population. **Sentinel performs a USIS Widescreen National Criminal/Sex Offender search, state specific misdemeanor and felony verifications based on addresses received from their personal Experian TRAC report by social security number, and five-panel drug-testing on its employees before hiring.** Sentinel maintains a company-wide drug-free policy that is clearly outlined prior to hiring with Sentinel as well as clearly posted in common work areas. All employees prior to hiring are subjected to a drug screening, and Sentinel conducts random testing based on reasonable cause. **These results can be provided to any requesting agency upon request.** Also, as a condition of employment with Sentinel, all potential employees must pass a written examination. Sentinel's review process ensures that the candidates meet all background, educational, and experience standards as set forth by contractual obligations. In the event of a misdemeanor, Sentinel can provide a release for the employee to provide permission to release the necessary information to the state regarding the specifics of the employee's event. **Sentinel does not hire or employ persons with felony convictions or misdemeanors with moral turpitude**. All of Sentinel's employees are thoroughly screened to ensure that its employees' backgrounds can be verified and that they can be trusted with access to corrections facilities, court offices, and confidential offender and agency records.
4.0	**SECTION D Monitoring Services**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
4.1	Monitoring Services	The Vendor shall provide toll-free telephone and facsimile numbers for the Agency staff to access the operators, technical support and customer service specialists at the Monitoring Center.	**Sentinel exceeds this requirement. Sentinel provides toll-free telephone and facsimile numbers for the agency staff to access operators, technical support, help desk and customer service specialists at the monitoring center. Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's**

			monitoring center. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are staffed and fully operational 24 hours a day.** Sentinel strives to resolve any customer inquiries promptly and on the first contact and the majority of technical problems are resolved through technical telephone support, through remote diagnostics, or through equipment replacement using the on-site spares. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, changing a participant's schedule, performing participant enrollments or entering data into the system. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and proactively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Account Management/Field Services personnel for customer enhancement requests, suggestions and ideas.

4.2	Monitoring Services	The Vendor must provide a staffed communication system utilizing an 800-telephone number an 800- number fax, and email access, available 24-hours per day, 365 days per year at no additional charge to the Agency for technical, analysis, and application assistance.	**Sentinel exceeds this requirement. Staffed customer service and technical support operators are available through a toll-free telephone numbers, toll-free facsimile numbers and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel strives to resolve any customer inquiries promptly and on the first contact and the majority of technical problems are resolved through technical telephone support, through remote diagnostics, or through equipment replacement using the on-site spares. Each monitoring center operator has the expertise to easily provide technical, analysis, and application assistance. **IMPORTANT SENTINEL ADVANTANGE: Continuity of Monitoring Services**: All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring outsource monitoring services/help desk services to third-party providers for both RF and Alcohol thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.)
4.3	Monitoring Services	The Vendor's Monitoring Center service must be able to tailor the level of alert notification to meet individual Agency needs or protocols.	**Sentinel meets this requirement.** Sentinel's monitoring service can tailor the level of alert notification to meet individual agency needs and protocols, including but not limited to all aspects of notification defined by this WSCA RFP. **SenTrak** provides many advanced features including the capability to determine notification protocol(s). Sentinel will work with the agency to determine and program appropriate agency notification profiles based on the type of program and level of risk to public safely of its participants. Each agency will have the capability to determine an agency specific level or levels of notification. Each authorized user within the agency will then have the ability to choose from the agency-determined notification protocols on a per participant basis. For example, an officer can choose to receive only an email notification of violations for a particular participant but may choose to receive a telephone call and an emailed report of the violation for a different participant. Additionally, individual users can choose to exclude certain events from

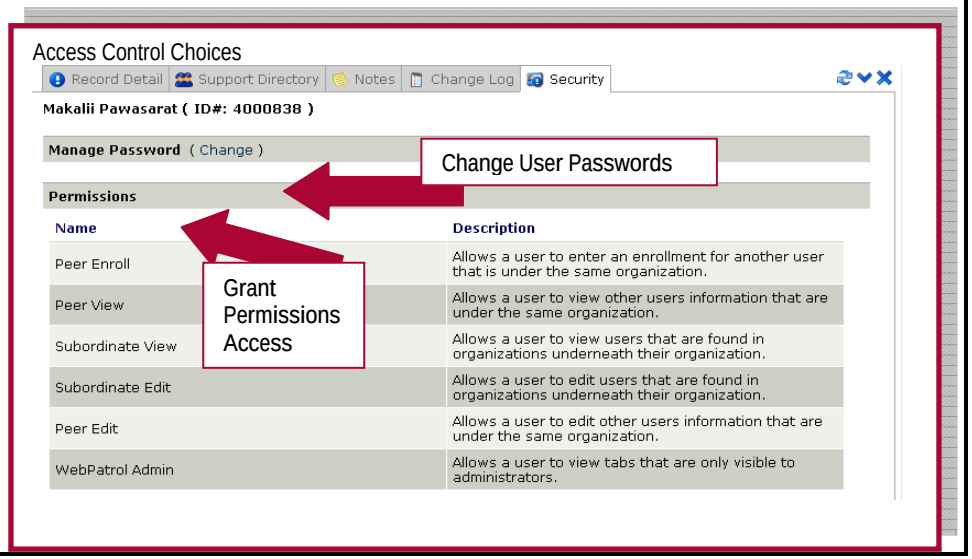
			notification if deemed unnecessary on a per participant basis. These events would still be included on daily, weekly or monthly reports. Notification methods can also vary by supervising personnel. **IMPORTANT SENTINEL ADVANTANGE: Sentinel monitoring services are ISO 9001:2008 certified** and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations **including agency/departmental specific operational procedures for monitoring, notification protocols, technical support and/or customer service.**
4.4	Monitoring Services	Describe in detail your 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. Describe system reporting and/or web-based capabilities to audit the notification steps taken for each alert.	**Sentinel exceeds this requirement.** Sentinel operates a highly unique automated system via toll-free 800 number for officers to call in and acknowledge receipt of an alert through the Automated Messaging System (AMS). The AMS enables officers secure use of touch tones to rapidly acknowledge receipt of an alert and stop ongoing escalation. The AMS also allows offices to immediately connect to a live monitoring center operator or, as always, officers who prefer to clear alerts via voice telephone call with a live operator may call Sentinel's monitoring center direct and toll free 24/7 to do so as an alternative to the AMS. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's AMS is complemented by web-based audit capabilities capable of tracking the performance of both Sentinel and the agency's staff/program regarding notification steps and response for each alert. Sentinel's software provides management information reports capable of querying the details related to alert response. Authorized users can perform web-based report queries on any alert(s) to determine: the number of notification steps taken, the contacts(s) and method(s) used to attempt notification and the individual who ultimately confirmed receipt of notification – each accompanied by the date/time of occurrence. This unique Sentinel capability provides unparalleled accountability for user agencies. Sentinel will implement maintaining a notification tree that will be utilized when contacting participating staff to report alarm notifications pursuant to established protocols. If an acknowledgment by one of the participating agency staff members is not made or received within a specified time frame, the alarm notification shall be automatically in the notification tree escalation process to a repeat method, a next method and/or a next contact for notification until receipt has been acknowledged.

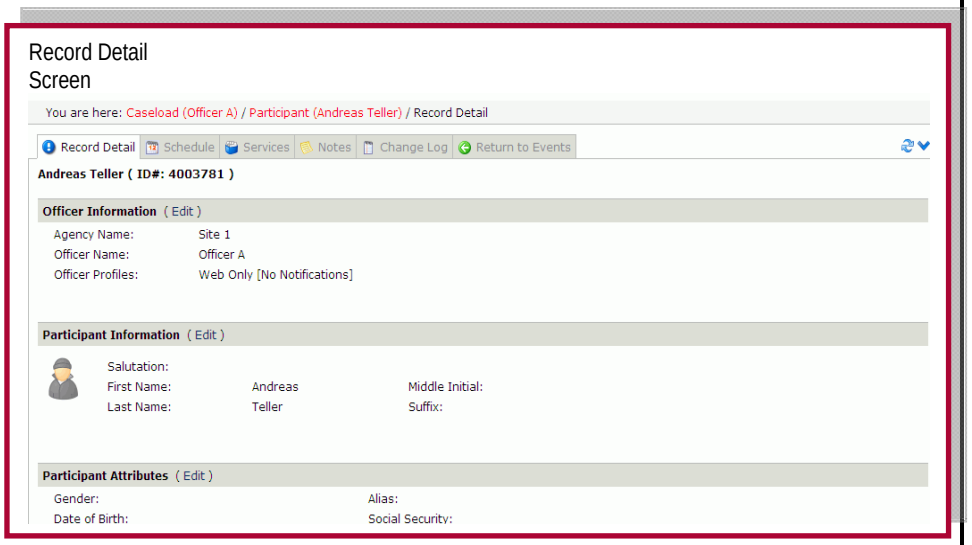
			IMPORTANT SENTINEL ADVANTAGE: Sentinel's monitoring software is highly unique in that it is designed and capable to specifically automate all steps except those the agency deems necessary and beneficial to be performed manually by a live monitoring center operator (example; call the participant) and to automate all other steps (dial, email, text, fax, track prescribed time-out intervals between notification steps, escalate to next contact/method, etc,) Furthermore, Sentinel's software can automatically alternate back and forth between automated notification steps and manual ones. This capability is unique to Sentinel significantly reducing the potential for human error thereby providing the fastest, most accurate notification available in the industry. Other vendors cannot alternate between automated and manual steps thus, once a manual step is called for, all subsequent notification steps must be performed solely by a live operator. **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record.
4.5	Monitoring Services	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:	**Sentinel meets this requirement.** Sentinel's SenTrak system and software provides secure (password-provided by the Sentinel) and protected internet or remote access to participant and monitoring information. Officers can complete a new participant enrollment including all relevant personal information for each participant, including all specified items. **Sentinel customers do not need to purchase or download any custom hardware or software.** At program inception, Sentinel assigns security passwords and unique login names to SenTrak users. SenTrak enables all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) to exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access. **IMPORTANT SENTINEL ADVANTAGE:** The SenTrak system provides administrative capability for managing a user's access level. The program administrator controls whether users have subordinate or peer-level access and assigns user names and passwords. Access can be set to a limited level where a user has access only to his or her caseload status or it can be set to a tiered-level, based on hierarchy of users and agency administrators. Typically, only

IMPORTANT SENTINEL ADVANTAGE: The SenTrak system provides administrative capability for managing a user's access level. The program administrator controls whether users have subordinate or peer-level access and assigns user names and passwords. Access can be set to a limited level where a user has access only to his or her caseload status or it can be set to a tiered-level, based on hierarchy of users and agency administrators. Typically, only senior level staff are assigned the highest access level, allowing access to all officers and all participant information and statuses. Regardless of the access level assigned, all users have access to the options for viewing, saving and/or printing data and/or reports, ensuring effective and efficient information exchange and report generation.

To make administrative changes to user access levels, an administrator selects the Access Control Choices option from his or her Module's Menu to display the Access Control Choices screen. From this screen, the administrator can select any individual user and select the user's Security Tab to perform the following administrative tasks:

- **Password Changes:** Click the (Change) option in the "Manage Password" column to change or reset passwords.
- **Permissions:** Click a permission option in the "Permissions" column to grant, change, or delete the level of user permissions.



4.6	Monitoring Services	a. Name, address, telephone number, equipment number, officer name, curfew information temporary and permanent schedule;	**Sentinel exceeds this requirement.** SenTrak supports a broad range of data elements that may be stored for each participant, including but not limited to: name, address, telephone number, equipment number, officer name, curfew information temporary and permanent schedule. Using SenTrak, officers can profile new participant enrollments for **RF Patrol®**. Sentinel has established basic entry requirements which include the participant's name, relevant addresses and phone numbers, supervising agency and officer information, along with monitoring device serial number(s) and service type. The SenTrak system also allows agencies to request customized fields for additional agency specific participant information. Sentinel is the original developer of SenTrak and Sentinel engineers control the web-based data fields, reports and queries, ensuring Sentinel is fully capable of meeting agency data and reporting needs. Record Detail Screen  As an additional benefit, users can enroll participants in the system and activate them at a later date. A user can view any saved enrollment on the Caseload Status screen in the Saved Enrollment section in SenTrak. Agency officers, equipment installers or authorized monitoring personnel can activate the saved enrollment upon notification of in-home equipment installation or on the participant's scheduled start date.

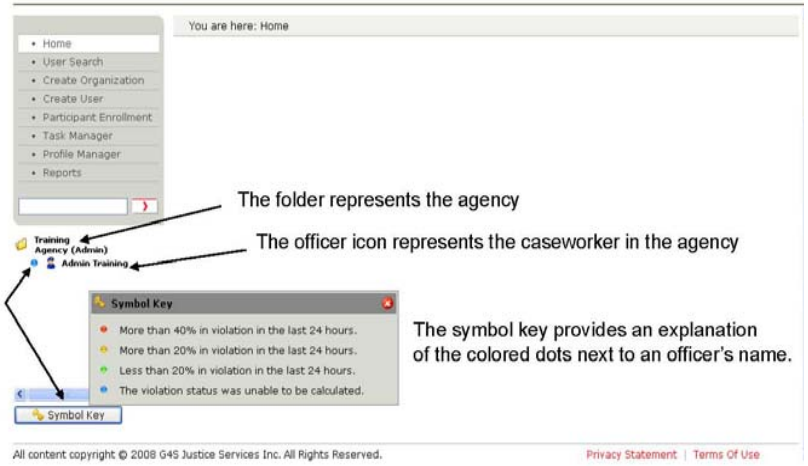
			During enrollment, Sentinel's software system also allows users to set curfew schedules on a per-participant basis, essentially establishing varying security levels. In other words, a user can assign riskier participants with stringent curfew schedules or less risky participant's lenient curfew schedules. The SenTrak software supports an unlimited number of curfew/absence periods per client, per day. Sentinel's advanced scheduler offers more options to better manage the variety of schedules within a user's caseload, such as: ▪ Permanent and temporary Schedules ▪ Curfew suspensions ▪ Lock down schedules ▪ Active and expired schedule availability ▪ Schedule conflict warnings A user is able to create schedules for RF monitoring participants through the simplified process by following these steps: (1) Select the appropriate days to which the schedule applies (2) Choose the start and end time, but only the start day and start time for an overnight schedule (3) Select the destination (4) Select the first box under the date if a participant will be absent for longer than a 24-hour time frame (5) Check the mandatory box if the participant MUST be out during this time frame Key features of the SenTrak Schedule Editor screen are: ▪ Check boxes provide a quick and easy process for selecting the appropriate days of the week to apply a participant's schedule. ▪ Overnight schedules require only a start day and start time unless a participant will be absent for longer than a 24-hour time frame. ▪ A clock function is available for selecting a schedule's start and end times, or the user can manually enter these times. ▪ The Destination drop-down menu provides a variety of standard monitoring destinations. ▪ A "mandatory" checkbox is available for the user to quickly indicate that the participant must be out during certain periods, including mandatory probation meetings or rehabilitation classes. ▪ Scheduling is flexible and comprehensive. A user can manually set up an override schedule for a participant needing to leave during a

			specified period of time or set up a permanent, temporary or mandatory schedule. After a user enters curfew periods, he or she can access the Monthly Schedule View screen to see a monthly view of the schedule. Any authorized user can print these monthly calendar-based schedules and use them when making field visits. The Monthly Schedule View features the following unique capabilities: ▪ The system uses easy–to-view symbol keys so officers can review schedules and destinations on a monthly, weekly or daily at-a-glance view. ▪ The system provides mouse-over capability that lets a user hover the mouse over the symbol key icon to view the schedule time and destination. The computer system immediately and automatically stores all of the data entered at the time of enrollment. SenTrak date and time stamps, and records the user login name for all remote data entries. If a user in the field opts to call information into the monitoring center, monitoring center staff will enter the information and store the entries with a date and time stamp and the name of the monitoring center associate. SenTrak has proven to increase efficiency, reduce data entry time, increase accuracy, and will provide the most cost effective and virtually paperless solution to Sentinel clients.
4.7	Monitoring Services	b. Data/Curfew changes;	**Sentinel exceeds this requirement.** Sentinel's SenTrak allows users to set curfew schedules on a per-participant basis, essentially establishing varying security levels. In other words, a user can assign riskier participants with stringent curfew schedules or less risky participant's lenient curfew schedules. The SenTrak software supports an unlimited number of curfew/absence periods per client, per day. Sentinel's advanced scheduler offers more options to better manage the variety of schedules within a user's caseload, such as: ▪ Permanent and temporary Schedules ▪ Curfew suspensions ▪ Lock down schedules ▪ Active and expired schedule availability ▪ Schedule conflict warnings A user is able to create schedules for RF monitoring participants through the simplified process by following these steps: (1) Select the appropriate days to which the schedule applies

			(2) Choose the start and end time, but only the start day and start time for an overnight schedule (3) Select the destination (4) Select the first box under the date if a participant will be absent for longer than a 24-hour time frame (5) Check the mandatory box if the participant MUST be out during this time frame Key features of the SenTrak Schedule Editor screen are: ▪ Check boxes provide a quick and easy process for selecting the appropriate days of the week to apply a participant's schedule. ▪ Overnight schedules require only a start day and start time unless a participant will be absent for longer than a 24-hour time frame. ▪ A clock function is available for selecting a schedule's start and end times, or the user can manually enter these times. ▪ The Destination drop-down menu provides a variety of standard monitoring destinations. ▪ A "mandatory" checkbox is available for the user to quickly indicate that the participant must be out during certain periods, including mandatory probation meetings or rehabilitation classes. ▪ Scheduling is flexible and comprehensive. A user can manually set up an override schedule for a participant needing to leave during a specified period of time or set up a permanent, temporary or mandatory schedule. After a user enters curfew periods, he or she can access the Monthly Schedule View screen to see a monthly view of the schedule. Any authorized user can print these monthly calendar-based schedules and use them when making field visits. The Monthly Schedule View uses easy–to-view symbol keys so officers can review schedules and destinations on a monthly, weekly or daily at-a-glance view. The system provides mouse-over capability that lets a user hover the mouse over the symbol key icon to view the schedule time and destination. SenTrak allows all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) to exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access.

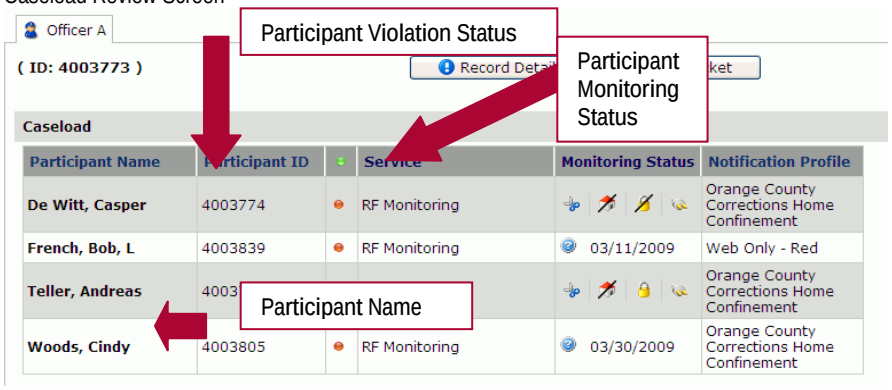
			IMPORTANT SENTINEL ADVANTAGE: The SenTrak system automatically logs all changes performed in SenTrak with the user's name, date and time of the change, and change the user made. Sentinel tracks **all** changes to the application, including but not limited to data and/or curfew changes, participant or agency details, notes, alert resolutions, enrollments, terminations and service requests. This information is viewable through the SenTrak Change Log and provides agencies with a clear audit trail for user accountability.
4.8	Monitoring Services	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;	**Sentinel meets this requirement.** Users have the ability to directly access participant information through Sentinel's SenTrak. The SenTrak system provides users with real-time access to participant events, daily statuses and caseload data including 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. Once logged in, authorized users including agency administrators are able to review their own caseload and participant statuses. To view a caseload from the Home Screen, users can click on his or her name on the Caseload Tree Legend found on the bottom left side of the screen. The Caseload Tree Legend is a hierarchical representation of the agency and individual agency users. Clicking on the user name will open the Caseload Review Screen to view caseload details.

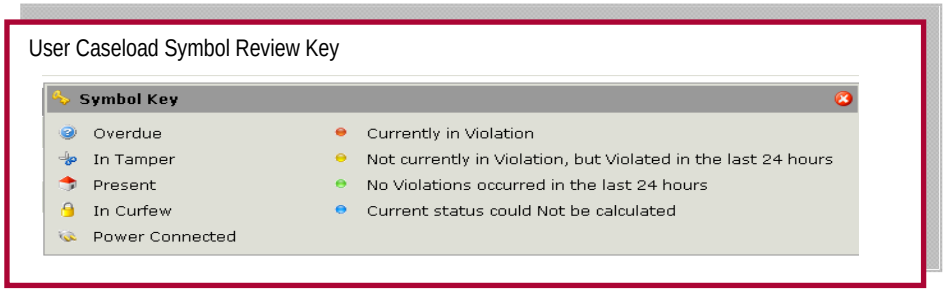
Caseload Tree Legend



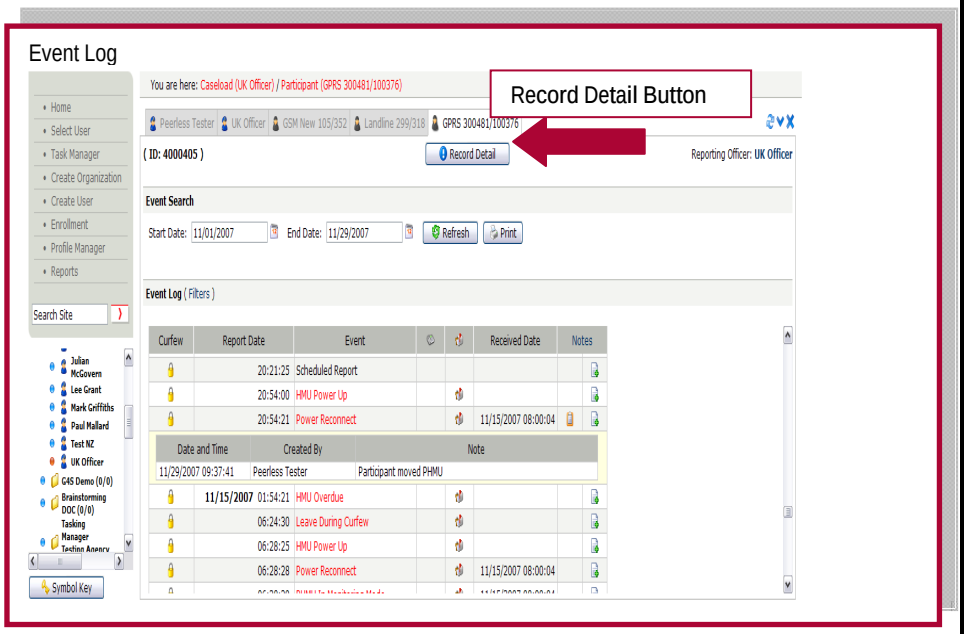
The "Caseload Review Screen" lists all participants for a user and utilizes two (2) columns featuring easy to recognize symbols to help quickly identify a participant's violation status and monitoring statuses.

Caseload Review Screen

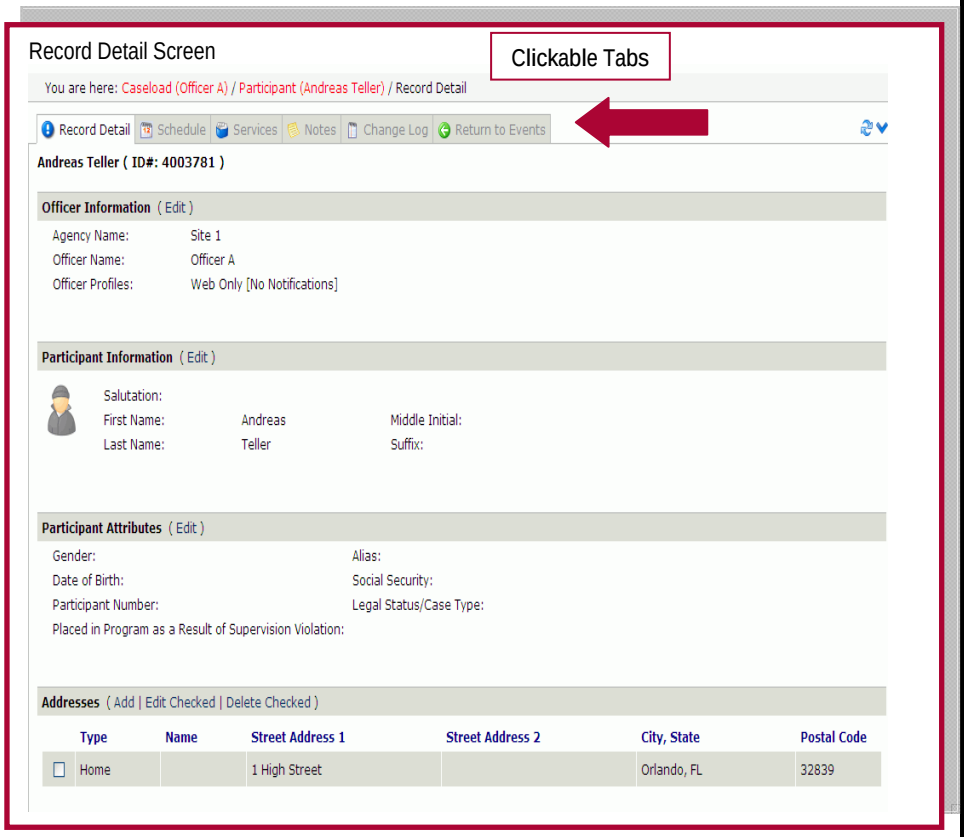




Clicking a participant's name in the Caseload Review Screen opens the Event Log screen where a user can view a participant's event log, monitoring statuses or alerts. This Event Log can be limited or expanded through the start date and end date fields.

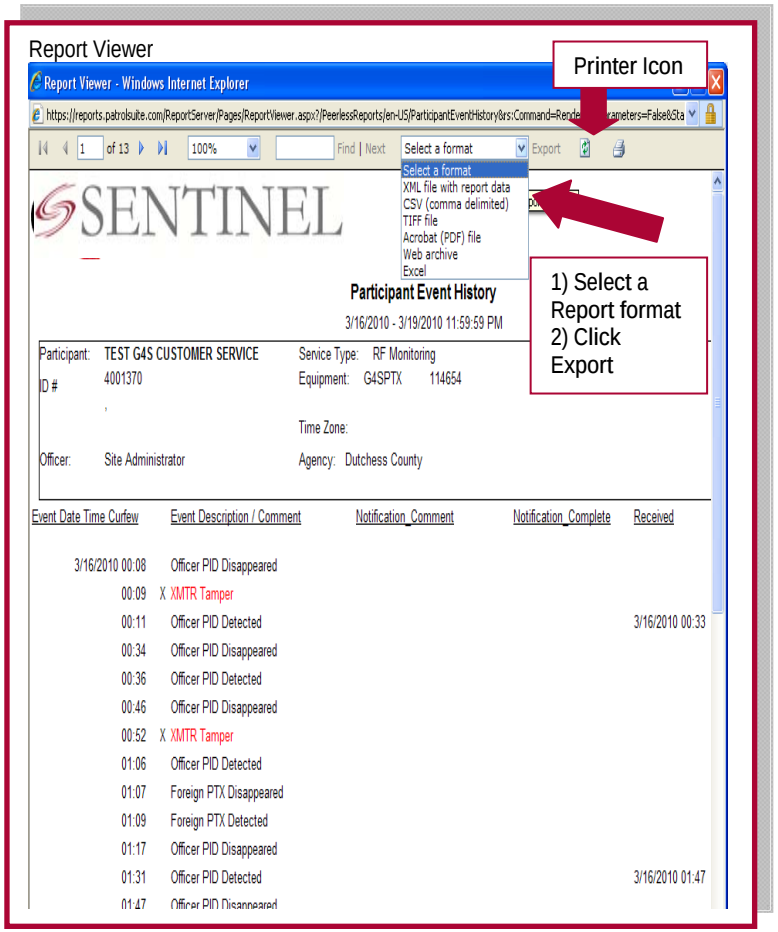


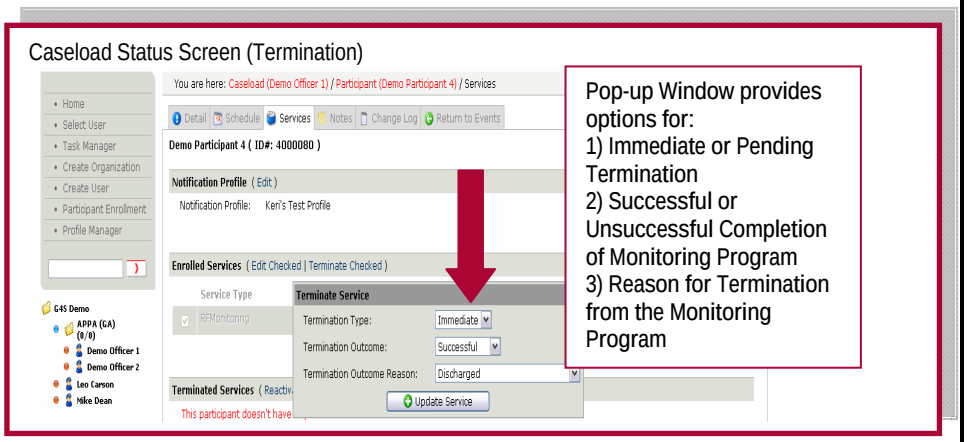
Clicking the Record Detail button on the Event Log screen opens the following Record Detail Screen where users can view a participant's enrollment record, or click one (1) of the tabs to display additional screens related to the participant's schedule, current services, notes, change log or simply to return to the Event Log.

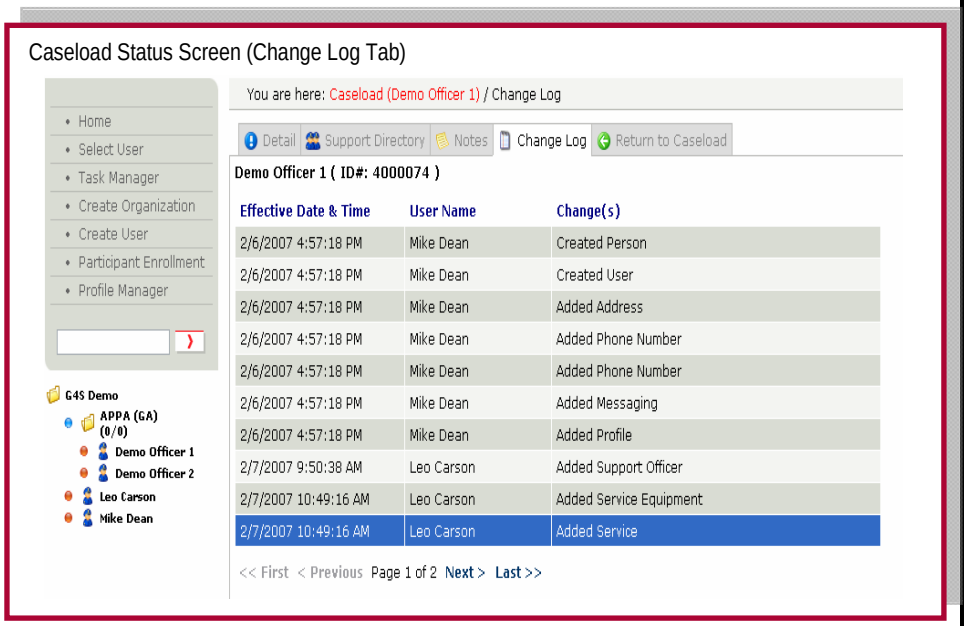
			
4.9	Monitoring Services	d. Report Analysis (e.g. Officers shall be able to generate and review monitoring/tracking reports on screen and print hard copies where necessary;	**Sentinel exceeds this requirement.** SenTrak provides authorized users with one of the largest libraries of web-based reports and queries available in the electronic monitoring industry – all at no additional charge. All monitoring reports are available through the easy-to-use report generator application of Sentinel's SenTrak software. Any authorized user can view participant activity 24 hours a day, seven (7) days a week, 365 days a year. Participant activity is posted **in real-time** so users can view violations online as they occur. Sentinel will work with its clients to ensure all needed reports, including on-demand, daily and quarterly reports are available.

			Based on requests from correction administrators for top-level program statistics, Sentinel developed custom software to extract broad level program data for custom reports. These optional reports provide program administrators the ability to analyze performance measurements on a statewide or countywide, per agency, per office and per caseload basis on demand basis or at regular specified intervals (commonly monthly, quarterly, semi-annually and annually). These optional reports have proven beneficial to program administrators as a means to better manage resources, identify trends in supervision and as a tool to balance caseloads among line staff. Some examples of the SenTrak reports are as follows: ▪ Active Inactive Inventory ▪ Active Participant Count ▪ Additions Deletions Report ▪ Agency Inactive Inventory ▪ Alarm Step History ▪ Alarm Step History by Participant ▪ Alerts Not Viewed ▪ Caseload by Participant ▪ Caseload Status ▪ Caseloads Not Viewed ▪ Caseloads Viewed ▪ Curfew Schedules ▪ Current Open Alarms ▪ Daily Status Exception ▪ Daily Status Report ▪ Daily Status Exception Report by Officer ▪ Daily Status Exception Report by Region ▪ Daily Status Exception Only Report by Officer ▪ Domestic Billing ▪ Domestic Billing by Type ▪ Drive-Bys ▪ Electronic Monitoring Participants en US ▪ EM Program Totals ▪ Equipment Last Call Date ▪ Inventory Returns ▪ Inventory Shipped to Agency ▪ Low Battery Status

			▪ No Leaves or Enters ▪ No Schedule Entered ▪ Notification History by Officer ▪ Officer Caseload ▪ Officer User Report ▪ Open Returns ▪ Organization Key Alerts ▪ Overdues ▪ Participant Not Home ▪ Participant Event History ▪ Participant Location Report ▪ Participant Notification History ▪ Participants Currently in Violation ▪ Schedule Out After Hours ▪ Tech Issues ▪ Termination Outcomes ▪ Violations Summary by Participant ▪ Web Only ▪ Enrolled Participant Roster greater than 60 days To export reports in SenTrak, users select a desired format including XML, CSV, TIFF, PDF, Web Archive and Excel and click Export. To print reports, users click the Printer Icon.

			
4.10	Monitoring Services	e. Terminate Participants (e.g. Officers shall be able to terminate monitoring/tracking on any participant on their caseload.)	**Sentinel meets this requirement.** Users have the ability to terminate a participant's monitoring through the SenTrak Caseload Screen on the Services Tab. Under the Enrolled Services menu, select the participant service to terminate and click on the Terminate Checked selection. The pop-up window provides authorized staff with the ability to force resolution when terminating clients from the system. Additionally, SenTrak users can schedule terminations for a time in the future. The following example displays a completed Termination Screen within the Sentinel SenTrak system.

			
4.11	Monitoring Services	The Vendor's Monitoring Center service shall maintain accurate and concise historical logs of all telephone, text message, emails and fax calls attempted and completed, including date, time, and the associated incident. The Vendor shall make these logs available to the Agency upon request. History shall be maintained for six (6) years after termination or expiration of the Agency's contract with the Vendor.	**Sentinel exceeds this requirement.** All telephone calls to and from the monitoring center are recorded for training and auditing purposes and are available for later playback. Additionally, the central computer system continuously receives and retains all data sent by each receiver, together with the date and time of each occurrence. **The SenTrak system automatically logs all changes performed in SenTrak with the user's name, date and time of the change, and change the user made.** Sentinel tracks **all** changes to the application, including but not limited to participant or agency details, notes, alert notifications attempted or completed (text message, email, call or fax), alert resolutions, enrollments, terminations and service requests. **This information is viewable through the SenTrak Change Log and provides agencies with a clear audit trail for user accountability.**

			
4.12	Monitoring Services	All curfew and equipment status alerts shall be reported to Agency 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 fax and/or telephone on an optional basis. Vendor must have the capability of reporting alerts after applying a defined Agency grace period for reporting designated events.	**Sentinel exceeds this requirement.** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately or upon expired grace period. All Sentinel curfew and equipment status alerts shall be reported to agency staff immediately or upon expired grace period. Sentinel has the capability of reporting alerts after applying a defined agency grace period for reporting designated events. Alerts can be reported by web-based system and/or email and alert reports may be provided in a variety of methods, including but not limited to: (alpha or numeric), electronic mail, manual voice phone call, fax, and/or text message to a cell phone. Sentinel confirms the Western States Contracting Alliance participating agencies will have the ability to customize notification profiles at the participant level. In fact, SenTrak provides many advanced features including the capability to determine notification protocol(s). Sentinel will work with the agency to determine and program appropriate agency notification profiles based on the type of program and level of risk to public safely of its participants. For example, an agency may choose to outline three (3) notification profiles:

			▪ Level 1: The user will receive event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through SenTrak. ▪ Level 2: The user will receive all tamper and curfew violations immediately by email and/or text message, all event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through SenTrak. ▪ Level 3: The user will receive all event notifications and alert violations immediately by email, text message, and/or manual voice message, and have access to view all participant event and alert information immediately through SenTrak. Please note that the notification levels previously described are examples only. Each agency will have the capability to determine an agency specific level or multiple levels of notification. Additionally, each authorized user within the agency will then have the ability to choose from the custom notification protocols on a per participant basis. For example, an officer can choose to receive only an email notification of violations for a particular participant but may choose to receive a telephone call and an emailed report of the violation for a different participant. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to include grace periods for specified violations before the system generates notification should the agency request this service.
4.13	Monitoring Services	The Vendor shall be capable of immediately notifying the designated Agency 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.	**Sentinel meets this requirement.** Sentinel will immediately notify the designated agency Program Manager verbally of any interruption in service or processing delay to the monitoring center or telecommunications systems lasting longer than 60 minutes 24 hours a day, seven (7) days a week, 365 days a year. Sentinel manages this through its System Performance Monitoring. A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure, the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction that are promptly routed to a live operator for verbal notification of predefined program administrators. Sentinel is prepared to provide this verbal notification to WSCA user agencies, as defined, based on telecommunications systems lasting longer than 60 minutes and perform such verbal notification 24 hours a day, seven (7) days a week, 365 days a year.

			IMPORTANT SENTINEL ADVANTAGE: Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Any instance of failure resulting in a loss of monitoring capability will be reported to the participating agency. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services.
4.14	Monitoring Services	The Vendor shall 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.	**Sentinel exceeds this requirement.** Sentinel maintains redundant inbound and outbound communication services, provided by distinct carriers such that the failure of the primary service or method does not adversely affect the secondary (backup) service or method. The Sentinel monitoring center features the following technology for its redundant Internet and telephone communications: ▪ T-1 telephone trunks, provided from three (3) redundant leading providers, to prevent against outages ▪ 432 Fiber-optic telecom cable lines and 200 POTS lines fed directly into the Sentinel facility ▪ Primary provider, Cox Communications (a leading provider of communications) is regionally headquartered within 8 miles and has triple electrical and data redundancy ▪ Second redundant carrier, AT&T ▪ Third redundant carrier, TW Telecom ▪ Cisco IP Telephony Solution combined with Cisco Networking for providing statistical tracking of all data and telephone activity A confidential, predefined and rehearsed protocol is set up with Sentinel's telecoms provider to enable a rapid transfer in accordance with the agreed service level. The back-up call handler functions in an active state and is ready to receive calls from the monitoring units as soon as the calls are rerouted from the primary call handler by Sentinel's Telecom providers.
4.15	Monitoring Services	The Vendor shall perform complete support of all interface hardware and software equipment (within the Monitoring Center) necessary to ensure provision of the service for the duration of the contract.	**Sentinel exceeds this requirement.** Support of all interface hardware and software equipment will be provided by Sentinel's team of full-time Information Technology (IT) personnel and equipment through its state-of-the-art monitoring facility located in Irvine California that houses the central computer system and monitoring personnel responsible for supporting the proposed solution. **Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support**

			operations, resolve any system issue, and ensure continued operations for the duration of the contract, including but not limited to interface hardware and software equipment within the monitoring center. **IMPORTANT SENTINEL ADVANTAGE:** To support operations for database replication of key IT, and failover disaster recovery to avoid unnecessarily excessive downtime due to hardware or software issues, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers are located in Atlanta, Georgia, over 500 miles apart. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. Redundant web servers, application servers and database servers, are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred.
4.16	Monitoring Services	The Vendor shall provide the Agency a contact number, accessible twenty (24) hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced.	**Sentinel meets this requirement.** Sentinel provides agencies with toll free phone and fax contact numbers, accessible24 hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced. Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center. All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Additionally, Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be**

			confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.
5.0	**SECTION E Alert Notifications**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
5.1	Alert Notifications	The Radio Frequency electronic monitoring system shall be capable of providing real-time and batch notification(s) to the Officer on the following violations/alerts:	**Sentinel exceeds this requirement.** SenTrak is capable of providing real-time and batch notification(s) to officers on the specified violations/alerts. Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately or upon expired grace period. Sentinel supports standard methods of notification, such page (alpha or numeric), electronic mail, manual voice phone call, fax, and/or text message to a cell phone. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to include grace periods for specified violations before the system generates notification should the agency request this service. Sentinel provides alert notifications for a wide array of alert violations and events notifications.
5.2	Alert Notifications	a. Non-compliance with pre-determined curfews;	**Sentinel meets this requirement.** Sentinel provides alert notifications for a wide array of non-compliance events with pre-determined curfews including:

Notification Exceptions	Description
Leave During Curfew	The participant's PTX2 has left the range of the PHMU during curfew.
Return During Curfew	The participant's PTX2 has come into range of the PHMU during curfew.
Curfew Start Present	The participant's Curfew has started and their PTX2 is present.
Curfew Start Not Present	The participant's Curfew has started and their PTX2 is not present.
Curfew Start Status Unknown	The participant's Curfew has started, but their PTX2 presence is unknown due to HMU Overdue

			Curfew Start Status Update-Present	The System processed the Curfew Start-Not Present status, the System received an Enter late that occurred prior to the Curfew Start, resulting in a 'Curfew Start Status Update-Present' event.
			Curfew Start Status Update-Not Present	The System processed the Curfew Start-Present status, the System received a Leave late that occurred prior to the Curfew Start, resulting in a 'Curfew Start Status Update-Not Present' event.
			Curfew Start Status Update-Review Events	The System processed either Curfew Start Status event, the System received three or more Leave/Enter events late that occurred prior to the Curfew Start status, resulting in 'Curfew Start Status Update-Present', 'Curfew Start Status Update-Not Present' event (order will depend on original status) and a 'Curfew Start Status Update-Review Events' event.
			Curfew End Present	The participant's Curfew has ended and their PTX2 is present.
			Curfew End Not Present	The participant's Curfew has ended and their PTX2 is not present
			Curfew End Status Unknown	The participant's Curfew has ended, but their PTX2 presence is unknown due to HMU Overdue
			Curfew End Status Update-Present	Enter late that occurred prior to the Curfew End, resulting in a 'Curfew End Status Update-Present' event
			Curfew End Status Update-Not Present	The System processed the Curfew End-Not Present status, the System received a Leave late that occurred prior to the Curfew End, resulting in a 'Curfew End Status Update-Not Present' event.

			Curfew End Status Update-Review Events — The System processed either Curfew End Status, the System received three or more Leave/Enter events late that occurred prior to the Curfew End, resulting in 'Curfew End Status Update-Present', 'Curfew End Status Update-Not Present' event (order will depend on original status) and a 'Curfew End Status Update-Review Events' event
5.3	Alert Notifications	b. Participant entry and exit at unauthorized times;	**Sentinel exceeds this requirement.** Sentinel provides alert notifications for **ALL** participant entry and exits including entry and exit at unauthorized times as shown on the following table:

Notification Exceptions	Description
Enter	The participant's PTX2 has come into range of the PHMU.
Leave	The participant's PTX2 has left the range of the PHMU.
Short Leave	The participant's PTX2 left the range of the PHMU for less than the leave window.
Enter During Mandatory Schedule	The participant's PTX2 has come into range of the PHMU during their Mandatory leave time.
Leave During Mandatory Schedule	The participant's PTX2 has left the range of the PHMU after they were required to be out.
Mandatory Schedule Start Present	The participant's Mandatory leave time has started and their PTX2 is present.
Mandatory Schedule Start Not Present	The participant's Mandatory leave time has started and their PTX2 is not present.
Mandatory Schedule Start Status Update-Present	The System processed the Mandatory Schedule Start-Not Present status, the System received an Enter late that occurred prior to the Mandatory Schedule Start, resulting in a 'Mandatory Schedule Start Status Update-Present' event.

			Mandatory Schedule Start Status Update-Present	The System processed the Mandatory Schedule Start-Not Present status, the System received an Enter late that occurred prior to the Mandatory Schedule Start, resulting in a 'Mandatory Schedule Start Status Update-Present' event.
			Mandatory Schedule Start Status Update-Not Present	The System processed the Mandatory Schedule Start-Present status, the System received a Leave late that occurred prior to the Mandatory Schedule Start, resulting in a 'Mandatory Schedule Start Status Update-Not Present' event.
			Mandatory Schedule Start Status Update-Review Events	The System processed either Mandatory Schedule Start status, the System received three or more Leave/Enter events late that occurred prior to the Mandatory Schedule Start, resulting in 'Mandatory Schedule Start Status Update-Present', 'Mandatory Schedule Start Status Update-Not Present' event (order will depend on original status) and a ''Mandatory Schedule Start Status Update-Review Events' event.
			Mandatory Schedule End Present	The participant's Mandatory leave time has ended and their PTX2 is present.
			Mandatory Schedule End Not Present	The participant's Mandatory leave time has ended and their PTX2 is not present.
			Mandatory Schedule End Status Update-Present	The System processed the Mandatory Schedule End-Not Present status, the System received an Enter late that occurred prior to the Mandatory Schedule End, resulting in a 'Mandatory Schedule End Status Update-Present' event.

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Mandatory Schedule End Status Update-Not Present</td><td>The System processed the Mandatory Schedule End-Present status, the System received a Leave late that occurred prior to the Mandatory Schedule End, resulting in a ‘Mandatory Schedule End Status Update-Not Present’ event.</td></tr>
<tr><td>Mandatory Schedule End Status Update-Review Events</td><td>The System processed either Mandatory Schedule End event, the System received three or more Leave/Enter events late that occurred prior to the Mandatory Schedule End status, resulting in ‘Mandatory Schedule End Status Update-Present’, ‘Mandatory Schedule End Status Update-Not Present’ event (order will depend on original status) and a ‘Mandatory Schedule End Status Update-Review Events’ event.</td></tr>
</table>
</td></tr>
<tr><td>5.4</td><td>Alert Notifications</td><td>c. Tampering with the transmitter or any of its components;</td><td>
Sentinel exceeds this requirement. Sentinel provides alert notifications for a wide array of transmitter tamper events including
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>XMTR Tamper</td><td>The PTX2 has detected a tamper and requires physical inspection.</td></tr>
<tr><td>XMTR Band Open</td><td>The PTX2 Band was open at the time of report from the PHMU and requires physical inspection.</td></tr>
</table>
IMPORTANT SENTINEL ADVANTAGE: When properly installed, participants cannot remove the transmitter without destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot stretch or slip off the PTX2 without detection. Following initial activation, RF Patrol® does not require unattended, automatic resetting of tamper alarms. It provides the capability for inspection of the band and clips and if determined necessary, agency personnel can use a unique key fob to disable, remove, inspect the back of the transmitter, and then reset the transmitter once the band is secure. A visual inspection produces a “Restart” event for the PTX2 bracelet, confirming that an authorized person has manually reset the device.
</td></tr>
</table>

			Please note that early generation electronic monitoring equipment without the advanced Sentinel straps suffer from two (2) problems: (a) tamper circuits that are stretchable and/or (b) tamper circuits that could potentially be mechanically circumvented. **Some vendor's have attempted to resolve these problems using "redundant tamper detection" including a primary "strap tamper" detection circuit with a secondary back-up "body tamper" or "proximity tamper" detection circuit in the same transmitter.** "Proximity" or "Body" sensors necessitate that the transmitter maintain constant contact with the skin, which is often impossible creating the potential for numerous nuisance false tamper alerts. It is common for the transmitter to momentarily break contact with the skin, perhaps while the participant is sleeping, bathing or simply slipping a sock or stocking underneath the transmitter, at which time the unit provides a "false tamper," that requires follow up either by state staff or monitoring center staff to attempt to validate if the "body" tamper is real or another false alert. Because of the number of false alerts and the unreliable nature of body sensors, many agencies choose to turn-off the "body" alert or ask the vendor not to notify them on these alarms, as they are unreliable. By attempting to resolve one problem; the "Proximity" / "Body" sensors created another. False tamper alarms jeopardize officer and participant confidence in the system and the program. Additionally, to Sentinel's knowledge, two (2) companies currently maintain body tamper technology and both only provide this technology in older generation radio frequency monitoring equipment. It is important to note, neither one of the two vendors currently utilizing this technology for radio frequency monitoring have included the "body tamper" technology in their latest generation one-piece GPS equipment. **Both companies have abandoned the "body tamper" technology in their one-piece GPS equipment, which historically is used on higher risk offenders.** Both companies have modified their GPS equipment to utilize the most reliable, proven and widely used method for tamper detection, fiber-optic tamper detection, similar to that which Sentinel has incorporated in the RF Patrol® equipment. In contrast to other vendors and in response to the previously described industry trend, Sentinel developed a superior tamper detection system for its **RF Patrol®** transmitter including a strap that is not stretchable and featuring a fiber optic light circuit that is not susceptible to manual circumvention. Sentinel transmitters have proven successful and corrections agencies that rely on the

			most accurate technology available have confidently used this fiber-optic circuitry worldwide including in the world's largest and arguably most intensive radio frequency monitoring program. The state-of-the-art design of the **RF Patrol®** transmitter has eliminated the need for a secondary and often faulty back up tamper detection system with one full reliable system. Sentinel's proposed **RF Patrol®** transmitter has the ability to detect and distinguish two (2) different types of tamper events that will provide the agency accurate tamper information. This unique technology eliminates the concern of "false tamper" alerts created through normal usage at home or in typical work environments because the PTX2 can only be properly installed by connecting both ends of the uniquely manufactured strap to the PTX2 with non-commercially available clips. **Proper installation of the devices only occurs once the fiber-optic circuit that runs through the center of the strap and through the PTX2 itself is completed.** **Sentinel Tamper Events:** (1) "Band Open": A "Band Open" event will only be produced if the band itself is cut or if the band is removed from the PTX2 casing through destruction of the non-commercially available clips used during installation therefore causing an on-going tamper condition. This alert is Sentinel's equivalent, **yet more technologically advanced,** alert to a "body tamper" and **will only occur due to true removal of the device**. As the band is not stretchable, a "band open" event will only be produced should the fiber-optic connections that run through **both** the strap and the transmitter be completely severed. (NOTE: It is impossible for the participant to properly reconnect an RF Patrol® PTX2 once the band is cut or the band is removed from the PTX2 casing as both the straps and clips are non-commercially manufactured.) (2) "Band Tamper": This alert is produced when the fiber-optic circuit running through the band and PTX2 is momentarily interrupted and then re-established indicating that the device has not been completely removed. NOTE: These unique tamper events are differentiated on SenTrak and on all agency reports.

<table>
<tr>
<td>5.5</td>
<td>Alert Notifications</td>
<td>d. Tampering with the Receiver or any of its components;</td>
<td>Sentinel meets this requirement. Sentinel provides alert notifications for a wide array of receiver tamper events including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>HMU Tamper</td><td>The PHMU has detected a tamper and requires physical inspection.</td></tr>
<tr><td>HMU Tilt</td><td>The PHMU has been continually moved for approximately 20 seconds or longer.</td></tr>
<tr><td>PHMU Forced Power Down</td><td>The PHMU has been manually powered down.</td></tr>
<tr><td>Power Disconnect</td><td>The electrical power supply has been disconnected from the PHMU.</td></tr>
<tr><td>Communication No Dial Tone</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to no dial tone.</td></tr>
<tr><td>Telephone Disconnect</td><td>The telephone line has been disconnected from the PHMU.</td></tr>
</table></td>
</tr>
<tr>
<td>5.6</td>
<td>Alert Notifications</td>
<td>e. Failure of the Receiver to report at pre-determined times;</td>
<td>Sentinel exceeds this requirement. Sentinel provides notifications for a wide array of events including both the success and failure of the receiver to report of pre-determined times, changes in report schedules and any immediate call-in request as shown in the following table:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>HMU Overdue</td><td>The PHMU is Overdue from making its scheduled report.</td></tr>
<tr><td>Scheduled Report</td><td>The PHMU made a regularly scheduled report to the Monitoring System.</td></tr>
<tr><td>PHMU Report Schedule Changed (Old, New)</td><td>The Scheduled Report Interval was changed within the PHMU menus</td></tr>
<tr><td>Immediate Call In Request</td><td>Sentinel sent a command to the PHMU instructing it to call back. Most commonly used when there is a programming change for the PHMU to acknowledge like Remote PTX2 Change.</td></tr>
</table></td>
</tr>
</table>

<table>
<tr><td>5.7</td><td>Alert Notifications</td><td>f. Loss and/or restoration of telecommunications;</td><td>Sentinel exceeds this requirement. Sentinel provides alert notifications for a wide array of loss and/or restoration of telecommunications events including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>Telephone Disconnect</td><td>The telephone line has been disconnected from the PHMU.</td></tr>
<tr><td>Telephone Reconnect</td><td>The telephone line has been connected to the PHMU.</td></tr>
<tr><td>Communication Circuits Busy</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to busy circuits.</td></tr>
<tr><td>Communication No Answer</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to no answer.</td></tr>
<tr><td>Communication Break</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to call interruption.</td></tr>
<tr><td>Communication No Dial Tone</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to no dial tone.</td></tr>
</table></td></tr>
<tr><td>5.8</td><td>Alert Notifications</td><td>g. Loss and/or restoration of alternating current (AC) power;</td><td>Sentinel meets this requirement. Sentinel provides alert notifications for a wide array of loss and/or restoration of alternating current (AC) power events including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>Power Disconnect</td><td>The electrical power supply has been disconnected from the PHMU.</td></tr>
<tr><td>Power Reconnect</td><td>The electrical power supply has been connected to the PHMU.</td></tr>
<tr><td>PHMU Forced Power Down</td><td>The PHMU has been manually powered down.</td></tr>
<tr><td>HMU Power Up</td><td>The PHMU has been powered up.</td></tr>
</table></td></tr>
</table>

<table>
<tr>
<td>5.9</td>
<td>Alert Notifications</td>
<td>h. Detection of low power or battery malfunctions in the transmitter or Receiver;</td>
<td>Sentinel meets this requirement. Sentinel provides alert notifications for a wide array of detection events of low power or battery malfunctions in the transmitter or receiver including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>XMTR Low Battery</td><td>The PTX2 battery is low and requires return to Sentinel.</td></tr>
<tr><td>HMU Low Battery</td><td>The PHMU backup battery is low and requires charging.</td></tr>
<tr><td>HMU Shutdown</td><td>The PHMU is powering down due to low battery.</td></tr>
</table>
</td>
</tr>
<tr>
<td>5.10</td>
<td>Alert Notifications</td>
<td>i. Movement of the Receiver to an unauthorized telephone line;</td>
<td>Sentinel exceeds this requirement. Sentinel provides alert notifications for a wide array of alert violations and events notifications including movement of the receiver to an unauthorized location.
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>HMU Unauthorized Telephone</td><td>The PHMU is reporting in from an unauthorized telephone number.</td></tr>
<tr><td>HMU Tilt</td><td>The PHMU has been continually moved for approximately 20 seconds or longer.</td></tr>
</table>
IMPORTANT SENTINEL ADVANTAGE: Both RF Patrol® units incorporate an industry-leading intelligent movement sensor known as “tilt detection” built-in that can aid the officer in differentiating between momentary movement and attempted relocation of the unit.</td>
</tr>
<tr>
<td>5.11</td>
<td>Alert Notifications</td>
<td>j. Detection of operating malfunctions in the Receiver or transmitter.</td>
<td>Sentinel meets this requirement. Sentinel provides alert notifications for a wide array operating malfunctions and internal diagnostics in the receiver both during monitoring initialization and routine operation of the equipment. During initial activation:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>Remote PTX2 Add</td><td>A PTX2 has been enrolled to the PHMU remotely.</td></tr>
<tr><td>Officer PID Detected</td><td>The PHMU has detected an OPID in its range.</td></tr>
<tr><td>Officer PID Disappeared</td><td>The PHMU is no longer detecting an OPID in its range.</td></tr>
<tr><td>Invalid Officer PID Detected</td><td>The PHMU has detected an invalid OPID in its range.</td></tr>
</table>
</td>
</tr>
</table>

Officer PID Out Of Sync	The OPID and PHMU may be out of sync. Repeat occurrences require further investigation.
PHMU In Officer Mode	The PHMU Menu Key has been turned to the Setup Mode.
PHMU In Monitoring Mode	The PHMU Menu Key has been turned to the Monitoring Mode.
Key To Menu Mode	The PHMU Menu Key has been turned to the Setup Mode.
Key to Officer Mode	The PHMU Menu Key has been turned to the Monitoring Mode.
HMU Enrollment	The enrollment process of the RF Equipment has begun.
HMU Installation Complete	The installation process of the RF Equipment is complete.

During monitoring:

Notification Exceptions	Description
HMU Diagnostics	The PHMU has provided internal operating and diagnostic information.
HMU System Source	The PHMU has provided internal operating and diagnostic information.
Out of Sync.	The PTX2 and PHMU may be out of sync. Repeat occurrences may require further investigation.
Remote PTX2 Change	The PTX2 being monitored has been changed remotely.
Remote PTX2 Remove	A PTX2 has been removed from the PHMU remotely.
Foreign PTX2 Detected	The PHMU has detected a foreign PTX2 in its range.
Foreign PTX2 Disappeared	The PHMU is no longer detecting a foreign PTX2 in its range.

5.12	Alert Notifications	Vendor shall have a notification policy for participant violations that allows the Agency to establish distinct levels of security on a participant by participant basis.	**Sentinel meets this requirement.** Sentinel confirms the Western States Contracting Alliance participating agencies will have the ability to customize notification profiles at the participant level. In fact, SenTrak provides many advanced features including the capability to determine notification protocol(s). Sentinel will work with the agency to determine and program appropriate agency notification profiles based on the type of program and level of risk to public safely of its participants. **Additionally, each authorized user within the agency will then have the ability to choose from the custom notification protocols on a per participant basis.** For example, an officer can choose to receive only an email notification of violations for a particular participant but may choose to receive a telephone call and an emailed report of the violation for a different participant. For example, an agency may choose to outline three (3) notification profiles: ▪ Level 1: The user will receive event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through SenTrak. ▪ Level 2: The user will receive all tamper and curfew violations immediately by email and/or text message, all event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through SenTrak. ▪ Level 3: The user will receive all event notifications and alert violations immediately by email, text message, and/or manual voice message, and have access to view all participant event and alert information immediately through SenTrak. Please note that the notification levels previously described are examples only. Each agency will have the capability to determine an agency specific level or multiple levels of notification. Additionally at no additional cost, Sentinel will customize each individual participating agency's notification profiles to include grace periods for specified violations before the system generates notification should the agency request this service.

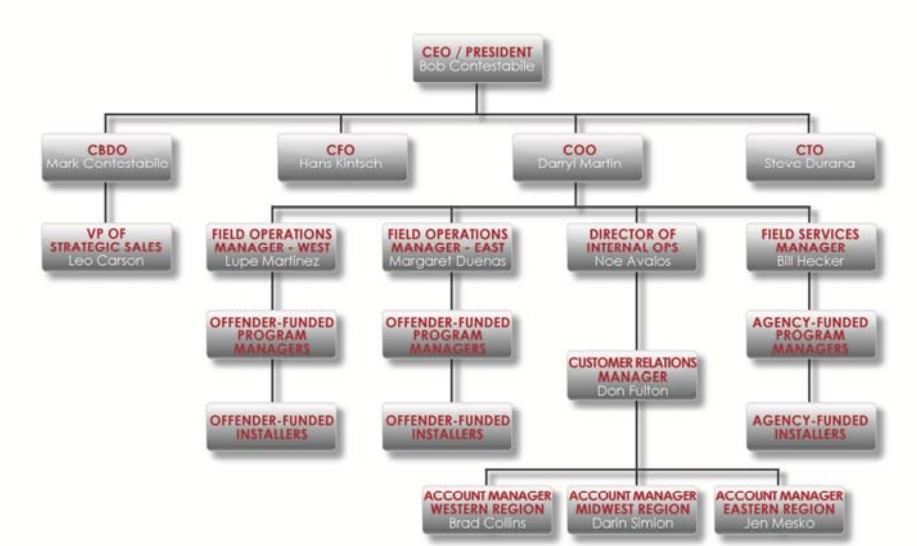
6.0	SECTION F Reports		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
6.1	Reports	Please provide a list of typical detailed reports the Vendor provides to current or previous customers.	**Sentinel meets this requirement.** SenTrak provides authorized users with one of the largest libraries of web-based reports and queries available in the electronic monitoring industry – all at no additional charge. All monitoring reports are (7) days a week, 365 days a year. Participant activity is posted **in real-time** so users available through the easy-to-use report generator application of Sentinel's SenTrak software. Any authorized user can view participant activity 24 hours a day, seven can view violations online as they occur. Sentinel will work with its clients to ensure all needed reports, including on-demand, daily and quarterly reports are available. SenTrak can provide the following radio frequency reports immediately or on an on-going basis. ▪ Active Inactive Inventory ▪ Active Participant Count ▪ Additions Deletions Report ▪ Agency Inactive Inventory ▪ Alarm Step History ▪ Alarm Step History by Participant ▪ Alerts Not Viewed ▪ Caseload by Participant ▪ Caseload Status ▪ Caseloads Not Viewed ▪ Caseloads Viewed ▪ Curfew Schedules ▪ Current Open Alarms ▪ Daily Status Exception ▪ Daily Status Report ▪ Daily Status Exception Report by Officer ▪ Daily Status Exception Report by Region ▪ Daily Status Exception Only Report by Officer ▪ Domestic Billing ▪ Domestic Billing by Type ▪ Drive-Bys ▪ Electronic Monitoring Participants en US ▪ EM Program Totals

			▪ Equipment Last Call Date ▪ Inventory Returns ▪ Inventory Shipped to Agency ▪ Low Battery Status ▪ No Leaves or Enters ▪ No Schedule Entered ▪ Notification History by Officer ▪ Officer Caseload ▪ Officer User Report ▪ Open Returns ▪ Organization Key Alerts ▪ Overdues ▪ Participant Not Home ▪ Participant Event History ▪ Participant Location Report ▪ Participant Notification History ▪ Participants Currently in Violation ▪ Schedule Out After Hours ▪ Tech Issues ▪ Termination Outcomes ▪ Violations Summary by Participant ▪ Web Only Enrolled Participant Roster greater than 60 days
6.2	Reports	Describe how the Vendor plans to provide the following reports should they be requested by Agency.	**Sentinel meets this requirement.** Unlimited access to all monitoring reports is available through the easy-to-use report generator application of Sentinel's SenTrak software or alternatively via email or fax upon request. Any authorized user can view participant activity 24 hours a day, seven (7) days a week, 365 days a year. Participant activity is posted **in real-time** so users can view violations online as they occur. Sentinel will work with its clients to ensure all needed reports, including on-demand, daily and quarterly reports are available. Additionally, Sentinel can provide customized optional reports to program administrators to analyze performance measurements on a statewide or countywide, per agency, per office and per caseload basis on demand basis or at regular specified intervals (commonly monthly, quarterly, semi-annually and annually).

6.3	Reports	a. Daily Utilization by Agency offices ;	**Sentinel meets this requirement.** Through the SenTrak software, Sentinel currently has two (2) standard reports that will provide each participating agency with information regarding the daily utilization by agency offices including: **Active Participant Count:** Lists participant counts by equipment type for State, Region and/or Office. **Caseload by Participant:** Caseload roster of participants sorted by office and then by officer Additionally, Sentinel can provide customized optional reports to program administrators to analyze performance measurements on a statewide or countywide, per agency, per office and per caseload basis on demand basis or at regular specified intervals (commonly monthly, quarterly, semi-annually and annually).
6.4	Reports	b. On-demand report containing the serial numbers of each Transmitter and Receiver in use, the participant's name and other Agency defined data.	**Sentinel exceeds this requirement.** Through the SenTrak software, Sentinel currently has a standard report that can be run on-demand or on a scheduled basis that will provide each participating agency with information regarding the serial numbers of each transmitter and receiver in use, the participant's name and other Agency defined data including: **Agency Active/Inactive Inventory:** Report containing the serial numbers of each PHMU, PTX **in use and inactive**. Report also identifies Key Fobs, OPID's and Drive-bys.
6.5	Reports	c. On-demand report containing the serial numbers of each Transmitter and Receiver not in In-Service Status	**Sentinel meets this requirement.** Through the SenTrak software, Sentinel currently has a standard report that can be run on-demand or on a scheduled basis that will provide each participating agency with information regarding the serial numbers of each transmitter and receiver not in in-service status including: **Agency Inactive Inventory:** Report containing the serial numbers of PHMU and PTX not in service status.
6.6	Reports	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;	**Sentinel exceeds this requirement.** Through the SenTrak software, Sentinel currently has a standard report that can be run on-demand or on a scheduled basis that will provide each participating agency with information regarding the serial numbers of each Transmitter, Receiver and Mobile Receiver (Drive-By) returned to the Vendor from each office during the report week including: **Inventory Returns:** Report containing serial numbers of equipment returned to Sentinel from each office.

			IMPORTANT SENTINAL ADVANTAGE: Sentinel also provides the following report detailing all equipment that has been shipping to the agency for reconciliation of received inventory. **Inventory Shipped to Agency:** Report containing serial numbers of equipment shipped to each office.
6.7	Reports	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;	**Sentinel meets this requirement.** Sentinel provides an on-demand (user defined date range) report containing the serial numbers of each transmitter, receiver and drive-by reported lost, absconded, stolen or not recovered from each region and office for specified periods. This Lost, Damaged, Stolen Equipment Report is provided on demand via email from the Sentinel monitoring center. Additionally, Sentinel Regional Account Managers monitor maintenance records concerning lost, absconded, stolen or not recovered equipment inventory and will provide any participating agency with a report containing this information on either a schedule or on-demand within 48 hours of request.
6.8	Reports	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;	**Sentinel meets this requirement.** Through the SenTrak software, Sentinel currently has a standard report that can be run on-demand or on a scheduled basis that will provide each participating agency with information regarding the serial number of each drive-by in the agency's possession during the report month that can be sorted by region and office including: **Drive Bys:** Listing of Drive bys by serial number and location.
6.9	Reports	g. Daily active Participant Roster Report.	**Sentinel meets this requirement.** Through the SenTrak software, Sentinel currently has a standard report that can be run on-demand or on a scheduled basis that will provide each participating agency with information regarding the daily active participant roster including: **EM Participants:** List of participants on electronic monitoring. Additionally, the SenTrak Caseload Management screen provides this data via the web-based system.
6.10	Reports	On-demand reports with user defined fields as requested by Agency.	**Sentinel meets this requirement.** Sentinel will provide customized optional on-demand reports with user defined fields as requested by the participating agency to assist with the monitoring of participants and/or the monitoring of program effectiveness. Based on requests from correction administrators for top-level program statistics, Sentinel developed custom software to extract broad level program data for custom reports. Sentinel can provide customized optional reports to

			program administrators to analyze performance measurements on a statewide or countywide, per agency, per office and per caseload basis on demand basis or at regular specified intervals (commonly monthly, quarterly, semi-annually and annually). These optional reports have proven beneficial to program administrators as a means to better manage resources, identify trends in supervision and as a tool to balance caseloads among line staff.
7.0	**SECTION G Account Management and Training**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
7.1	Account Management	The Vendor shall assign staff to provide adequate training and explanation to Agency staff regarding the maintenance, use, and care of the radio-frequency EM monitoring system equipment.	Sentinel exceeds this requirement. Sentinel has both a dedicated Training Department and assigned Regional Account Managers capable to provide adequate training and explanation to Agency staff regarding the maintenance, use, and care of the radio-frequency monitoring system equipment. IMPORTANT SENTINEL ADVANTAGE: As the incumbent provider of electronic monitoring radio frequency electronic monitoring services to the Western States Contracting Alliance and its participating agencies, Sentinel has an in-depth proven relationship with the participating agencies and understands their procedures and goals better than any other vendor in the industry. Additionally, participating agencies' staff currently working with Sentinel through the Western States Contracting Alliance contract are thoroughly familiar with and knowledgeable of the equipment and software being proposed in this response. Sentinel's extensive depth of field services personnel (as shown on the following organizational chart) will provide corporate oversight for the contractual cycle of each of the participating programs during the program lifecycle. The assigned field services personnel will be dispatched to provide on-site service in the event of the need for electronic diagnosis or replacement of component problems. Field services personnel will also be responsible for scheduling and providing training and explanation to participating agency staff regarding the maintenance, use, and care of the radio-frequency electronic monitoring system equipment, per the contract. This strong nation-wide presence of qualified Sentinel staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract. The following is a Key Personnel Organizational Chart followed by descriptions of the associated project tasks of Operational Staff responsible for this contract.

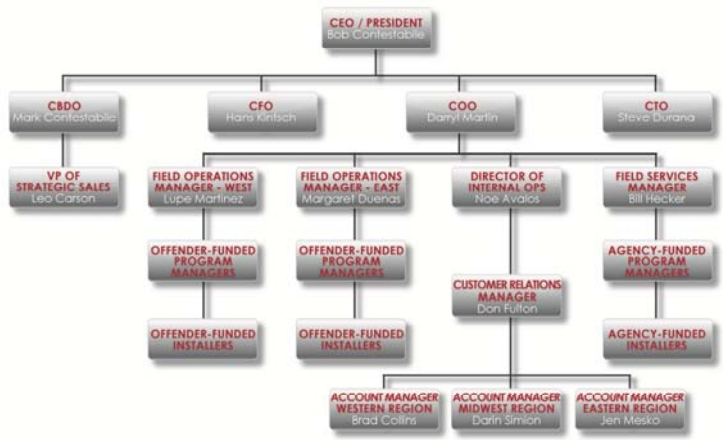


Sentinel has a proven track record of providing excellent performance and flexibility to its customers and will commit this same dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all services including but not limited to technical assistance, customer support, inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value.

IMPORTANT SENTINEL ADVANTANGE: **Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness.

Additionally, staffed monitoring services and technical support are available from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident**

			that Sentinel is experienced and fully capable of providing the necessary agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.
7.2	Account Management	The Vendor shall provide an Inventory Control Plan / Reports subject to Agency 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 any requesting agency post award.	Sentinel meets this requirement. Sentinel has an established inventory control plan and reports in place to maintain accurate inventory of both active and spare equipment at each agency it serves. Sentinel will provide each participating agency with a monthly and/or weekly (depending on agency preference) report of all inventory (both active and spare) in their possession. Sentinel will customize a report for each participating agency with any agency-specific information requests. Sentinel will work with participating agencies to maintain a thorough inventory against the complete list of all equipment and report back to Sentinel any non-functional, lost, absconded, stolen or not recovered equipment. Sentinel will replace all equipment reported. Additionally, should the spare equipment totals exceed the allotted spare equipment allowance, Sentinel will request and coordinate return/relocation of any excess equipment to Sentinel's warehouse. Sentinel's current inventory control plan consists of the following: ▪ A monthly and/or weekly (depending on agency preference) radio frequency equipment inventory report is distributed to the participating agency's inventory control person that identifies active, inactive and in transit RF equipment by type and location as well as all units returned to Sentinel identified by type and location. ▪ Each participating agency submits a monthly and/or weekly (depending on agency preference) lost, absconded, stolen or not recovered to Sentinel for tracking and billing purposes. ▪ Each participating agency submits a monthly and/or weekly (depending on agency preference) recovered equipment report to Sentinel for tracking and billing purposes. ▪ The participating agency's inventory control person reports any inventory discrepancies identified for their agency directly to Sentinel Account Manager for follow up.

7.3	Account Management	Vendor shall provide a liaison to the Agency that 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 Agency 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.	**Sentinel meets this requirement.** Sentinel has both a dedicated Training Department and assigned Regional Account Managers to ensure Contract services are provided at a satisfactory level including but not limited to: on-site on-going training to current Agency and new employees; technical assistance as requested; resolve issues and ensure customer satisfaction and perform customer support may include site visits and assistance with implementation of new phases of electronic monitoring program. Sentinel's extensive depth of field services personnel (as shown on the following organizational chart) will provide corporate oversight for the contractual cycle of each of the participating programs during the program lifecycle to resolve issues and ensure customer satisfaction, conduct site visits and provide assistance with implementation of new phases of electronic monitoring program. Each participating agency will be assigned a liaison field services staff member that will be dispatched to provide on-site service in the event of the need for technical assistance, electronic diagnosis or replacement of component problems. Field services personnel will also be responsible for scheduling and providing on-site initial and on-going training to participating agency staff regarding the maintenance, use, and care of the radio-frequency electronic monitoring system equipment, per the contract. This strong nation-wide presence of qualified Sentinel staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract. The following is a Key Personnel Organizational Chart followed by descriptions of the associated project tasks of Operational Staff responsible for this contract. 

			Sentinel has a proven track record of providing excellent performance and flexibility to its customers and will commit this same dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all services including but not limited to technical assistance, customer support, inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value. **IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness.
7.4	Training	Vendor shall provide initial on-site training by experienced staff with-thirty (30) days of start of Agency's contract, unless an alternate training schedule is agreed upon. Additional on-site training via webinar shall be provided within 48 hours of request. Ongoing training shall be provided as agreed mutually between vendor and agency.	**Sentinel meets this requirement.** Sentinel will provide initial on-site training by experienced staff within 30 days of start of agency's contract, unless an alternate training schedule is agreed upon. Additional on-site training via webinar will be provided within 48 hours of request. Ongoing training will be provided as agreed mutually between Sentinel and each agency. Sentinel is committed to working in partnership with each participating agency utilizing the Western States Contracting Alliance contract over the term of the contract to make sure that all staff are fully and properly trained on the operation and installation of the proposed equipment, the use of the software for participant management, and interpretation of violation notifications and reports along with all other needed training requirements. Sentinel will provide initial on-site training has included a sample written training curriculum in the Exhibits section of this proposal for the Western States Contracting Alliance to review and consider. Initial on-site training will be enacted prior to the implementation of the services. In Sentinel's experience, initial training should be conducted in near-proximity to intended program start date and be conducted to ensure that all agency personnel are completely comfortable and knowledgeable in using the proposed equipment and systems therefore Sentinel will provide initial training within thirty (30) days of the Notice to Proceed commencement date, unless an alternate training schedule is agreed upon. Initial training includes instruction on the operation of any monitoring equipment and software discussed in this proposal and selected for use and implementation by the respective participating agency. Once Sentinel

			management and participating agency management agree upon program guidelines, notifications, and parameters, Sentinel will arrange for a mutually beneficial training session. Additionally, Sentinel will provide post-deployment on-going training per the established contract at no cost to the participating agency. Any future training will be scheduled in a manner that is beneficial and cost-effective to both the agency and Sentinel. **IMPORTANT SENTINEL ADVANTAGE:** The Sentinel training department offers webinar training sessions for customers and staff on an on-going basis. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
7.5	Training	Vendor will provide training and/or user manuals in soft format (such as PDF) and shall authorize Agency to duplicate these materials as necessary to facilitate Agency training needs.	**Sentinel meets this requirement.** Sentinel will supply all operational, procedural and training materials, including written instructions and equipment for initial training, to be used by participating agency personnel at no additional cost. Sentinel will also provide all training and/or user manuals in soft format (such as PDF) and provide written authorization to the participating agency to duplicate these materials as necessary to facilitate future agency training needs.
7.6	Training	Deleted	

7.7	Training	Describe your company's capability to provide training both on-line and via Webinar.	**Sentinel meets this requirement.** Sentinel has both a dedicated Training Department and assigned Regional Account Managers capable to provide adequate training and explanation to Agency staff regarding the maintenance, use, and care of the radio-frequency monitoring system equipment. The Sentinel training department offers a variety of on-line and webinar training sessions for customers and staff on an on-going basis. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training
			within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
8.0	**SECTION H General Equipment, Transmitter and Receiver Specifications**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**

8.1	Equipment	Vendor is bidding the following device as a part of its Radio Frequency (RF) Continuous Signaling Electronic Monitoring Service and has identified this same device in the Price Worksheets. The responses to these specifications are for this equipment. **Body-attached Transmitter:** Mfg.: _____ Brand/Model: _____ **Receiver (Home Unit) – with Landline Connection:** Mfg.: _____ Brand/Model: _____ **Receiver (Home Unit) – with Cellular Communication:** Mfg.: _____ Brand/Model: _____	**Sentinel meets this requirement.** **Body-attached Transmitter:** Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol® PTX2 **Receiver (Home Unit) – with Landline Connection:** Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol® Landline PHMU **Receiver (Home Unit) – with Cellular Communication:** Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol® Cellular PHMU
8.2	Equipment	The equipment manufacturer shall have an ISO 9001 certification.	**Sentinel exceeds this requirement.** Much of Sentinel's success hinges on Sentinel's top management's commitment to continual process improvements, which is a main goal of the ISO 9001:2008 Quality Standard. **Sentinel's manufacturing division received ISO 9001-2008 accreditation in January 2009 and maintains this certification.** Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments and to ensure all staff has access to needed resources and training to support the quality management system. Sentinel has provided copies of the certifications in the Exhibits section of this proposal.

8.3	Equipment	The Vendor shall provide radio-frequency electronic monitoring equipment which shall be the most current and updated version of the Vendor's equipment. In addition, the Vendor must originally have purchased this equipment from the manufacturer. The Vendor's clients may have used the equipment as long as the Vendor was the original purchaser. All equipment must be clean and "like new" condition, damage free, and in acceptable operative order. Vendor shall 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.	**Sentinel meets this requirement.** Sentinel is pleased to propose **RF Patrol®**, its latest generation (the most current and updated version) Radio Frequency (RF) electronic monitoring technology platform. Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including the proposed **RF Patrol®** electronic monitoring solution. The **RF Patrol®** technology platform is supported by Sentinel's web-based information exchange, SenTrak. Sentinel will supply the Western States Contracting Alliance participating agencies clean and "like new" equipment that is damage free, and in acceptable operative order. Sentinel does not anticipate the discontinuation of any of the proposed products / technologies / services during the initial term of the contract.
8.4	Equipment	Equipment must be specifically designed as a Radio Frequency (RF) system equipment and shall not be derivative components from another tracking system.	**Sentinel meets this requirement. RF Patrol®** is specifically and uniquely designed for house arrest monitoring therefore is not made of derivative components from another tracking system.
8.5	Equipment	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.	**Sentinel exceeds this requirement.** The first two (2) elements of the highly advanced and secure system known as **RF Patrol®** include the following: ▪ PTX2: Personal Transmitter (can be paired with either Landline or Cellular PHMU units) ▪ PHMU: Personal Home Monitoring Unit (Landline or Cellular) **RF Patrol®** provides reliable home supervision to monitor the presence/absence of the transmitter within a specified range of the receiver. When in range, the PHMU automatically identifies the PTX2 and its current status and reports that status to the monitoring center via landline or cellular communications. This solution provides intensive heightened notification including the reporting of all changes in status including unauthorized absences, late returns, equipment malfunctions and tamper alerts. **IMPORTANT SENTINEL ADVANTAGE:** The following chart highlights the technology advantage of Sentinel transmitters over other companies in the industry:

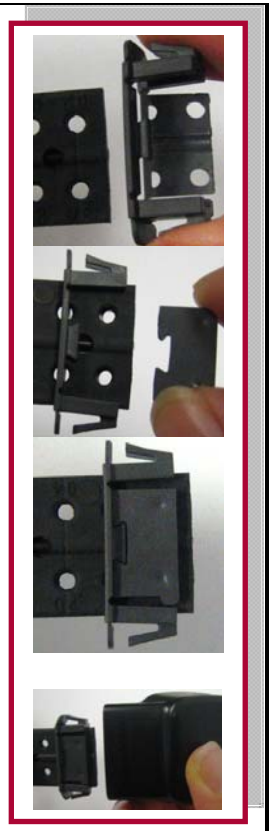
Transmitter Features	RF Patrol® PTX2
Participant Worn Device	Unique watch-size transmitter device for wrist or ankle
Device Specifications	Smallest and lightest available on the market at 1.57 X 2.72 X 0.77 inches and 1.51 ounces Waterproof and shockproof 100% humidity resistant
Tamper Alert	Yes, patented multiple fiber-optic circuits
Transmitter Battery Life	Designed for two (2) years with proactive scheduled replacement at 18 months in-use, four (4) year shelf life LED light indicating low battery life
Activation	On-site programmable range during installation (no software required)
Deactivation	Shutdown of transmitter via two-way RF link
Required Assembly of Transmitter	Easiest to install in the industry Transmitter is a sealed unit Four (4) easy to install transmitter pieces
Transmission Signal	Transceiver two-way communications technology (both a transmitter and receiver of signals) Unique semi-spherical antenna Variable transmission range of 50, 100 or 150 feet

IMPORTANT SENTINEL ADVANTAGE: Sentinel recognizes the growing trend of offenders to do away with landline home phone lines. To directly address this need, Sentinel is pleased to propose the most secure radio frequency models offered in the industry, including **RF Patrol® Landline** and **RF Patrol® Cellular**. Sentinel is pleased to offer two (2) models of **RF Patrol®** receiver/monitor units. The **RF Patrol® Landline** PHMU communicates all reports to the monitoring center via a landline communications network. Sentinel also offers an **RF Patrol® Cellular** PHMU that communicates all reports to the monitoring center via the wireless communications network.

IMPORTANT SENTINEL ADVANTAGE: The following chart highlights the technology advantage of Sentinel' PHMUs over other companies in the industry:

PHMU Features	RF Patrol® Landline	RF Patrol® Cellular
Device	Fully integrated one (1) piece unit Dual antennas and transceivers	Fully integrated one (1) piece unit Dual antennas and transceivers
PHMU Specifications	Smallest and lightest available on the market at 7.5 X 8.6 X 1.7 inches and weighs 16 ounces 100% humidity resistant	Smallest and lightest available on the market at 7.5 X 8.6 X 1.7 inches and weighs 16 ounces 100% humidity resistant
Tamper Alert	Yes, including tilt detection	Yes, including tilt detection
Back-up Battery Life	48 hours of continuous operation	48 hours of continuous operation
Front Panel LED Display Activation	Provides setup prompts for enrollment through LED display On-site programmable range testing during installation (no software required) Reports battery life of the PTX2 on screen	Provides setup prompts for enrollment through LED display On-site programmable range testing during installation (no software required) Reports battery life of the PTX2 on screen
Deactivation	Shutdown of transmitter (PTX2) via two-way RF link	Shutdown of transmitter (PTX2) via two-way RF link
Required Assembly	None	None
Transmission Signal	Transceiver technology with the PTX2 Landline communication with the monitoring center	Transceiver technology with the PTX2 Wireless cellular communication with the monitoring center

			Multiple Transmitters — Ability to monitor up to 50 PTX2s at the same time — Ability to monitor up to 50 PTX2s at the same time **Guest Detection** — Detects and reports unauthorized PTX2 units in range — Detects and reports unauthorized PTX2 units in range **Memory/Storage** — Internal non-volatile memory capable of storing 90 days of events indefinitely — Internal non-volatile memory capable of storing 90 days of events indefinitely
8.6	Equipment	Transmitters and Receivers shall be field replaceable and interchangeable without the need to return them to the Vendor.	**Sentinel meets this requirement.** Upon activation, the each **RF Patrol®** PHMU automatically identifies the PTX2 in range and synchronizes itself and the PTX2 as a matched set. As such, each PTX2 and PHMU are interchangeable components, enabling easy replacement of either component without replacement of the entire system.
8.7	Equipment	Installation process must be simple enough to be performed in the field by fully trained officers in less than 5 minutes. Describe such features to simplify Officer installation.	**Sentinel exceeds this requirement.** Any trained personnel can install the **RF Patrol®** PTX2 and PHMU in the participant's home (or applicable base monitoring location) in less than five (5) minutes. **IMPORTANT SENTINEL ADVANTAGE: Sentinel's PTX2 bracelet is the easiest to install in the industry. PTX2 uses only four (4) pieces for installation one-third-less pieces than required by other vendors like BI, Inc. whose transmitter requires the assembly of up to 12 pieces.** The Sentinel PTX2 transmitter is easily installed on the participant with minimal training and experience of the installer.

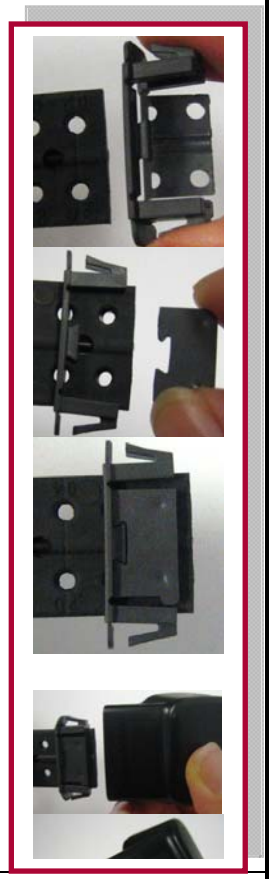
			Step 1: Prepare the PTX2 ▪ Insert end of the Band that has clip pre-attached into one end of the PTX2 housing ▪ Listen for two clicks to ensure the band is properly engaged Step 2: Sizing the PTX2 ▪ Wrap the PTX2 around the participants ankle until snug ▪ Measure to the closest hole to the edge of the face of the PTX2 ▪ Once the appropriate fit is established, remove the PTX2 from the participant and use the Guillotine Cutting Tool to cut the Band Step 3: Attaching the PTX2 to the Ankle ▪ Slide the Clip over the trimmed end of the Band until the holes on the Clip are aligned with the holes on the Band ▪ Apply the Pin to the available side of the Clip through the holes of the Band and press firmly until it locks into place and both the Clip and Pin are flush ▪ Wrap PTX2 Band around ankle of participant ▪ Insert this end of the Band into one end of the PTX2 housing ▪ Listen for two clicks to ensure the band is properly engaged  In the interest of public safety, Sentinel believes that it is it's crucial to keep detailed information regarding the installation of **RF Patrol®** from participants. Therefore, please see the **CONFIDENTIAL** **RF Patrol®** Landline and Cellular PTX2 Quick Reference Guide included in Exhibits section of this proposal for more detailed diagrams and an itemized list reflecting each and every part required to assemble the transmitter from the point it is received until it is installed on the offender.

8.8	Equipment	System must be designed with heightened emphasis on accuracy of RF signaling & speed of reporting. Describe unique design features that ensure accuracy and/or speed of reporting (Example: Use of 2-way radio transceivers instead of simple 1-way transmitter/receiver signaling).	**Sentinel exceeds this requirement.** The **RF Patrol®** PTX2 emits a unique (individually coded), constantly changing signal **on average approximately every 18 seconds**. **In fact, the RF Patrol® PTX2 is actually a transceiver to ensure accuracy of RF signaling and speed of reporting.** Sentinel developed and designed the PTX2 with innovative state-of-the-art two-way radio signal capability. This feature allows the PTX2 to communicate with the home monitoring unit and also allows the PHMU to communicate back to the PTX2 to confirm receipt of the signal in a range up to 150 feet. In contrast, other vendor's systems only offer one-way transmissions from the transmitter to the receiver. Through utilizing a two-way radio signal, the **RF Patrol®** system eliminates problems that plague other radio frequency monitoring systems, such as dead zones, hit or miss signaling, and false alerts. This technology has improved accuracy and provides faster overall notification. **IMPORTANT SENTINEL ADVANTAGE: Dual Transceiver, Two-way RF Link Approach:** Sentinel' unique dual transceiver approach incorporates both a transmitter and receiver in the PHMU, as well as having both in the PTX2. In fact, the **RF Patrol®** PHMU has two (2) constantly active internal antennas capable of both receiving from and transmitting signals to the PTX2 to maximize the ability to detect the presence of transmitter signals. For the first time in the industry, the two (2) components truly communicate with each other, automatically confirming alerts in advance of reporting. **RF Patrol's®** signaling is robust, fast and intelligent. The units can complete a closed loop signal confirmation **up to three (3) times in one (1) second**, resulting in the most sophisticated and reliable signaling in the industry. Some of the unique features of this innovative transceiver approach are: ▪ **Intelligent two-way transceiver technology** ▪ State-of-the-art Frequency Shift Keying (FSK) transceiver-based design ▪ Compliance with all applicable United States and International requirements ▪ Dual Transceiver with multi-path mitigation ▪ Acknowledgment of message delivery (PHMU will send acknowledgment to PTX2)

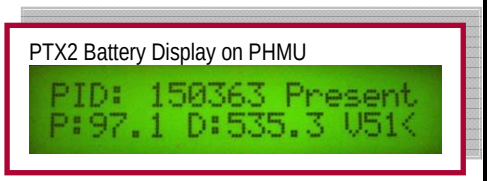
			▪ Robust over-the-air (OTA) radio protocol, checksums and automatic retries ▪ Bidirectional protocol enabling the PTX2 to know: ✓ When it's in "range test mode" through a blinking light on the PTX2 on successful message delivery ✓ When it's in range of the PHMU and conserves power when out of range ✓ Information used to optimize RF communications
8.9	Equipment	The Vendor shall 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 the Agency and after successful field testing of the updated system.	**Sentinel meets this requirement. Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Radio Frequency electronic monitoring contractor for more than 11 years since the WSCA contract's inception and proven to advance technologies to WSCA customers.** Sentinel will replace the radio-frequency electronic monitoring system with any future updated and improved version of Sentinel's radio-frequency electronic monitoring system on the request of the agency and after successful field testing of the updated system. Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including the proposed **RF Patrol®** electronic monitoring solution and SenTrak monitoring platform. As technology constantly changes, Sentinel strives to maintain its radio-frequency electronic monitoring equipment and software at the highest levels of performance. If future versions of the proposed hardware or software are released, Sentinel will implement the necessary changes after presenting the improvements to the participating agency with a thorough demonstration/field test of the new products and at the request of the agency. Sentinel will only provide Western States Contracting Alliance participating agencies with upgrades / improvements that have successfully been released.
8.10	Transmitter	Device must not pose a safety hazard or unduly restrict the activities of the participant. Must be light weight, small and water-resistant.	**Sentinel exceeds this requirement.** The **RF Patrol®** personal transmitter unit (PTX2) is lightweight and small at **just 1.57 X 2.72 X 0.77 inches and weighs just 1.51 ounces**. The unobtrusive, hypoallergenic and sleek PTX2 design makes it one of the smallest body-worn transmitter units available on the market. It is easily, securely and comfortably attached to the ankle of participants under normal slacks. It waterproof to 30 feet and does not pose a safety or health threat to the wearer or unduly restrict the activities of the participant.
8.11	Transmitter	The transmitter shall be encased in a water-resistant case that is corrosion resistant and impervious to chemical solvents and detergents.	**Sentinel meets this requirement.** The **RF Patrol®** PTX2 manufactured as a completely seal unit that is moisture and waterproof to 30 feet, corrosion resistant, impervious to chemical solvents and detergents, shock resistant, and unaffected by all normal human environmental and atmospheric conditions.

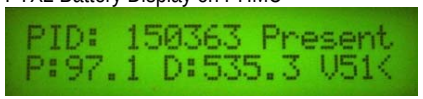
8.12	Transmitter	The transmitter shall be designed to prevent tracing or duplication of its signal.	**Sentinel exceeds this requirement.** To prevent interference, tracing or duplication of the radio frequency signal, the **RF Patrol®** transmitter signal has a 24-bit data string with more than four **(4) million** unique combinations. This design prohibits duplication of the signal (two different offenders sending the same message for one another via the same receiver) or interference from other RF signals commonly found in homes. The RF transmissions are the most reliable, sophisticated, and highly encrypted in the industry, and incorporate the following advanced security features:
8.12	(Continued		▪ **Frequency Alterations:** The **RF Patrol®** transmitter signal features a patented circuit and is designed to discourage tracing or duplicating by automatically and constantly changing the PTX2 transmission pulse rates (unique to each transmitter) during every other pulse to provide added protection against signal duplication and/or frequency interference. ▪ **Encrypted Radio Transmissions:** The **RF Patrol®** transmitter uses more than **four (4) million** unique transmission combinations. The constantly changing pulse rate is unique for each active transmitter, making it virtually impossible to predict or duplicate through the use of counterfeit transmitters or other radio equipment. The PHMU is aware and anticipates how each specific transmitter will vary transmissions. **No other electronic monitoring companies have currently incorporated this intelligence into their radio frequency monitoring systems units or devices.**
8.13	Transmitter	The transmitter shall have FCC approval for home use. Proposals should include the FCC approval number.	**Sentinel meets this requirement.** All of the proposed equipment complies with all appropriate FCC regulations. Sentinel has provided the transmitter FCC Identifier Numbers below and copies of all the RF Patrol® certifications are included in the Exhibits section of this proposal: **Part 15** ▪ RF Patrol® PTX NSNPTX08 **Part 68** ▪ RF Patrol® US:YEVMM06BPHMUL08
8.14	Transmitter	The Vendor shall provide either multi-length or sizeable transmitter straps with replacements provided at no additional cost to the Agency. (May be required to supply up to 4 disposable type straps per unit per year).	**Sentinel meets this requirement.** Sentinel provides varying length sizeable straps designed to fit any ankle size and that are easily replaceable in the field. Sentinel will provide replacements at no additional cost to the agency up to four (4) disposable straps per unit per year.

8.15	Transmitter	The transmitter shall be easily installed on the Participant with minimal training and experience. Vendor shall specify the tools required and procedures to install the transmitter. The Vendor shall supply the tools and equipment necessary to install the transmitters and replace the transmitter straps, at no additional cost. At least one tool kit will be included for each 25 units in use.	**Sentinel exceeds this requirement.** Agency personnel can easily install the **RF Patrol®** PTX2 with minimal training and experience. Sentinel will supply at least one tool kit for each 25 units in use and all equipment necessary to install the transmitters and replace the transmitter straps, at no additional cost. **IMPORTANT SENTINEL ADVANTAGE: Sentinel's PTX2 bracelet is the easiest to install in the industry. PTX2 uses only four (4) pieces for installation one-third-less pieces than required by other vendors like BI, Inc. whose transmitter requires the assembly of up to 12 pieces.** The Sentinel PTX2 transmitter is easily installed on the participant with minimal training and experience of the installer.

			Step 1: Prepare the PTX2 ▪ Insert end of the Band that has clip pre-attached into one end of the PTX2 housing ▪ Listen for two clicks to ensure the band is properly engaged Step 2: Sizing the PTX2 ▪ Wrap the PTX2 around the participants ankle until snug ▪ Measure to the closest hole to the edge of the face of the PTX2 ▪ Once the appropriate fit is established, remove the PTX2 from the participant and use the Guillotine Cutting Tool to cut the Band Step 3: Attaching the PTX2 to the Ankle ▪ Slide the Clip over the trimmed end of the Band until the holes on the Clip are aligned with the holes on the Band ▪ Apply the Pin to the available side of the Clip through the holes of the Band and press firmly until it locks into place and both the Clip and Pin are flush ▪ Wrap PTX2 Band around ankle of participant ▪ Insert this end of the Band into one end of the PTX2 housing ▪ Listen for two clicks to ensure the band is properly engaged 
			In the interest of public safety, Sentinel believes that it is it's crucial to keep detailed information regarding the installation of **RF Patrol®** from participants. Therefore, please see the **CONFIDENTIAL RF Patrol®** Landline and Cellular PTX2 Quick Reference Guide included in Exhibits section of this proposal **for more detailed diagrams and an itemized list reflecting each and every part required to assemble the transmitter from the point it is received until it is installed on the offender.**

<table>
<tr><td>8.16</td><td>Transmitter</td><td>Neither the transmitter, receiver, straps, fasteners nor clips, etc. used to install the transmitter shall be available to the general public.</td><td>Sentinel meets this requirement. Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including the proposed RF Patrol® electronic monitoring solution. Sentinel confirms that transmitter, receiver, straps, fasteners nor clips, etc. (or respective component parts) used to install the equipment are NOT commercially available to the general public.</td></tr>
<tr><td>8.17</td><td>Transmitter</td><td>At least seven (7) days prior to battery failure, the transmitter shall emit a low battery message to the Receiver and to the Monitoring Center, and shall be handled as a notifiable event.</td><td>Sentinel exceeds this requirement. Sentinel provides alert notifications for a wide array of detection events of low power or battery malfunctions in the transmitter or receiver including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>XMTR Low Battery</td><td>The PTX2 battery is low and requires return to Sentinel.</td></tr>
</table>
This alert will be emitted by the transmitter to the receiver and subsequently to the monitoring center At least seven (7) days prior to battery failure.

IMPORTANT SENTINEL ADVANTAGE: Sentinel is proposing its advanced transmitter (PTX2) which provides added confidence of reliable monitoring. This improved PTX2 continuously reports the remaining battery life to the Personal Home Monitoring Unit (PHMU) ensuring the agency will never be surprised by transmitter battery depletion. Agency personnel will have the ability during device installation or subsequent participant home visits to check the remaining battery life of the PTX2 directly through the Liquid Crystal Display (LCD) on the PHMU. As the example illustrates, the transmitter's remaining battery life is shown on the PHMU's LCD display reflecting current remaining power of 97.1% ("P: 97.1") and remaining battery life of 535.3 days ("D: 535.3"). Agency personnel can view this display through the simple process of selecting the INFO Menu on the PHMU's main display, then selecting Next to scroll to the Enrolled PTX2

</td></tr>
<tr><td></td><td></td><td></td><td>options. The officer would then select VIEW to access the enrolled PTX2 serial numbers, their presence, percentage and number of days of battery power remaining, and firmware version.</td></tr>
</table>

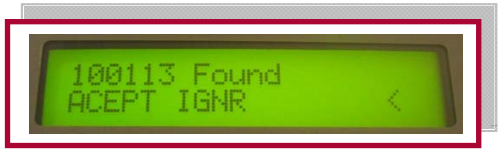
8.18	Transmitter	The transmitter battery should have a minimum of two (2) year active life and a three (3) year shelf life.	**Sentinel meets this requirement.** The PTX2 is powered by a lithium thionyl-chloride, 3.6V, 750 milliamp hours (mAh) battery pack that is designed for a continuous operating life of two (2) years and a four (4) year shelf life however, Sentinel supplies and specifies proactive replacements of PTX transmitters through officer's attritional in-office contact with offenders at an 18 month interval in order to proactively reduce officer field time associated with replacement. The **RF Patrol®** transmitter unit is manufactured as a completely sealed unit to provide a reliable battery life. The sealed unit ensures longer battery life by prohibiting leakage and eliminating the need for assembly during device installation. If the battery depletes, Sentinel will provide a replacement PTX2 at no cost. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's PTX2 battery life is nearly twice that of other vendors like BI, Inc. whose transmitter battery thereby resulting in significantly more officer in-field maintenance of their equipment. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel is proposing its advanced transmitter (PTX2) which provides added confidence of reliable monitoring. This improved PTX2 continuously reports the remaining battery life to the Personal Home Monitoring Unit (PHMU) ensuring the agency will never be surprised by transmitter battery depletion. Agency personnel will have the ability during device installation or subsequent participant home visits to check the remaining battery life of the PTX2 directly through the Liquid Crystal Display (LCD) on the PHMU. As the example illustrates, the transmitter's remaining battery life is shown on the PHMU's LCD display reflecting current remaining power of 97.1% ("P: 97.1") and remaining battery life of 535.3 days ("D: 535.3"). Agency personnel can view this display through the simple process of selecting the **INFO Menu** on the PHMU's main display, then selecting **Next** to scroll to the **Enrolled PTX2** options. The officer would then select **VIEW** to access the enrolled PTX2 serial numbers, their presence, percentage and number of days of battery power remaining, and firmware version. PTX2 Battery Display on PHMU 

8.19	Transmitter	The transmitter shall feature multiple levels of tamper detection capable of detecting disassembly of the transmitter case and/or cutting or circumventing of the transmitter strap.	**Sentinel exceeds this requirement.** The **RF Patrol's®** transmitter features multiple levels of tamper detection capable of detecting disassembly of the transmitter case and/or cutting or circumventing of the transmitter strap. **RF Patrol's®** sophisticated fiber-optic strap design uses light rather than a conductive circuit to ensure the participant cannot tamper with the unit without the generation of a tamper report. The 16 individual tamper detection circuits embedded in the strap send a pulse of light through the fibers at a rate faster than once every second, constantly confirming the status of the strap. **RF Patrol®** will immediately notify the host computer (when in range of the receiver) of any tamper attempt or removal from the offender's ankle. Sentinel transmitters have proven successful and corrections agencies that rely on the most accurate technology available have confidently used this fiber-optic circuitry worldwide. This unique technology eliminates the concern of "false tamper" alerts created through normal usage at home or in typical work environments. When properly installed, participants cannot remove the transmitter without destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot stretch or slip off the PTX2 without detection. Following initial activation, **RF Patrol®** does not allow unattended, automatic resetting of tamper alarms. It does provide the capability for inspection of the band and clips and if determined necessary, agency personnel can use a unique key fob to disable, remove, inspect the back of the transmitter, and then reset the transmitter once the band is secure. A visual inspection produces a "Restart" event for the PTX2 bracelet, confirming that an authorized person has manually reset the device. **IMPORTANT SENTINEL ADVANTAGE:** Please note that early generation electronic monitoring equipment without the advanced Sentinel straps suffer from two (2) problems: (a) tamper circuits that are stretchable and/or (b) tamper circuits that could potentially be mechanically circumvented. **Some vendor's have attempted to resolve these problems using "redundant tamper detection" including a primary "strap tamper" detection circuit with a secondary back-up "body tamper" or "proximity tamper" detection circuit in the same transmitter.** "Proximity" or "Body" sensors necessitate that the transmitter maintain constant contact with the skin, which is often impossible creating the potential for numerous nuisance false tamper alerts. It is common for the transmitter to momentarily break contact with the skin,

			perhaps while the participant is sleeping, bathing or simply slipping a sock or stocking underneath the transmitter, at which time the unit provides a "false tamper," that requires follow up either by state staff or monitoring center staff to attempt to validate if the "body" tamper is real or another false alert. Because of the number of false alerts and the unreliable nature of body sensors, many agencies choose to turn-off the "body" alert or ask the vendor not to notify them on these alarms, as they are unreliable. By attempting to resolve one problem; the "Proximity" / "Body" sensors created another. False tamper alarms jeopardize officer and participant confidence in the system and the program. Additionally, to Sentinel's knowledge, two (2) companies currently maintain body tamper technology and both only provide this technology in older generation radio frequency monitoring equipment. It is important to note, neither one of the two vendors currently utilizing this technology for radio frequency monitoring have included the "body tamper" technology in their latest generation one-piece GPS equipment. **Both companies have abandoned the "body tamper" technology in their one-piece GPS equipment, which historically is used on higher risk offenders.** Both companies have modified their GPS equipment to utilize the most reliable, proven and widely used method for tamper detection, fiber-optic tamper detection, similar to that which Sentinel has incorporated in the RF Patrol® equipment. In contrast to other vendors and in response to the previously described industry trend, Sentinel developed a superior tamper detection system for its **RF Patrol®** transmitter including a strap that is not stretchable and featuring a fiber optic light circuit that is not susceptible to manual circumvention. Sentinel transmitters have proven successful and corrections agencies that rely on the most accurate technology available have confidently used this fiber-optic circuitry worldwide including in the world's largest and arguably most intensive radio frequency monitoring program. The state-of-the-art design of the **RF Patrol®** transmitter has eliminated the need for a secondary and often faulty back up tamper detection system with one full reliable system. Sentinel's proposed **RF Patrol®** transmitter has the ability to detect and distinguish two (2) different types of tamper events that will provide the agency accurate tamper information. This unique technology eliminates the concern of "false tamper" alerts created through normal usage at home or in typical work environments because the PTX2 can only be properly installed by connecting both ends of the uniquely manufactured strap to the PTX2 with non-commercially available clips. **Proper installation of the devices only occurs**

			once the fiber-optic circuit that runs through the center of the strap and through the PTX2 itself is completed. **Sentinel Tamper Events:** (1) "Band Open": A "Band Open" event will only be produced if the band itself is cut or if the band is removed from the PTX2 casing through destruction of the non-commercially available clips used during installation therefore causing an on-going tamper condition. This alert is Sentinel's equivalent, **yet more technologically advanced,** alert to a "body tamper" and **will only occur due to true removal of the device**. As the band is not stretchable, a "band open" event will only be produced should the fiber-optic connections that run through **both** the strap and the transmitter be completely severed. (NOTE: It is impossible for the participant to properly reconnect an RF Patrol® PTX2 once the band is cut or the band is removed from the PTX2 casing as both the straps and clips are non-commercially manufactured.) (2) "Band Tamper": This alert is produced when the fiber-optic circuit running through the band and PTX2 is momentarily interrupted and then re-established indicating that the device has not been completely removed. NOTE: These unique tamper events are differentiated on SenTrak and on all agency reports.
8.20	Transmitter	The transmitter shall be capable of storing and/or recording a tamper event that occurs out-of- range of the Receiver or Mobile Receiver Unit when the transmitter returns within range of either. The tamper attempt shall be communicated along with a time/date stamp.	**Sentinel meets this requirement.** The **RF Patrol®** transmitter is capable of storing and/or recording a tamper event that occurs out-of- range of the PHMU receiver or mobile receiver unit (**RF Patrol® Drive-By**) when the transmitter returns within range of either. The tamper attempt is communicated along with a time/date stamp. If a participant attempts to cut the fiber-optic strap **or remove** the unit, the unit automatically activates a "tamper alert" signal and continually transmits the "tamper alert" on an average of approximately once every 18 seconds. Should the participant be out of range of the home monitoring unit, the PTX2 will continue to transmit the "tamper alert" signal until it comes into range of the home monitoring unit and receives closed-loop confirmation that the home monitoring unit has received the tamper signal. The PHMU will immediately report the tamper alert along with a time/date stamp of its occurrence to the monitoring center upon arrival of the PTX2 in range. The monitoring center will additionally record a separate time/date stamp of

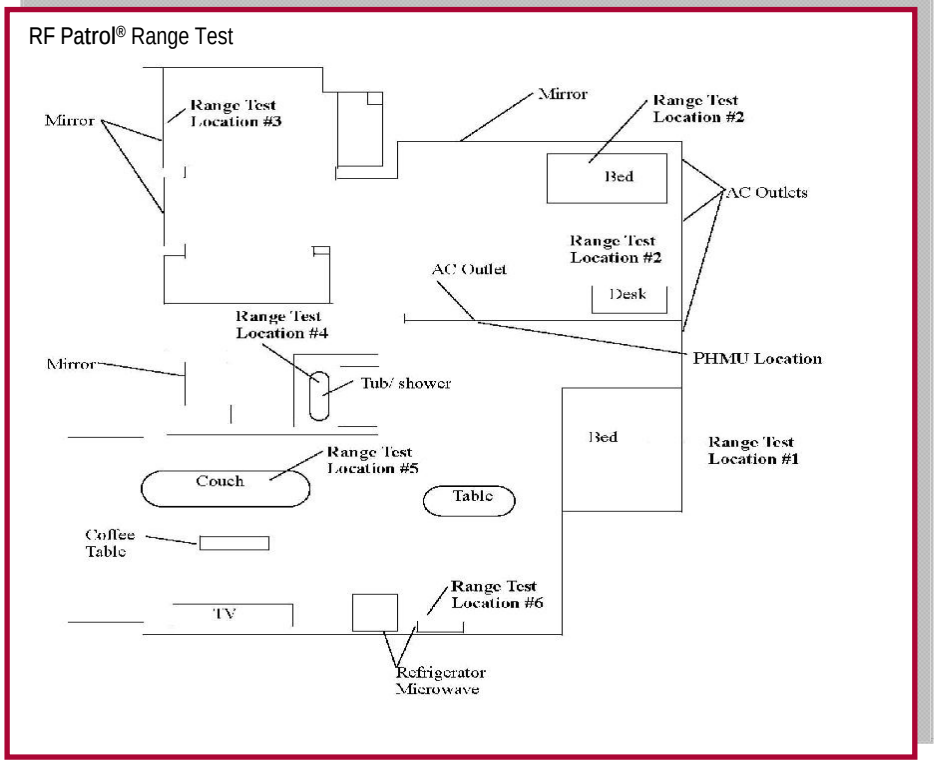
			indicating the receipt of the event. Additionally, each RF Patrol® Drive-by device (mobile receiver unit) detects and identifies all **RF Patrol®** transmitter (PTX2) signals in 300 to 500+ feet open field range and determines the condition of the transmitter including tamper and battery status of the PTX2.
8.21	Receiver	Receiver must be easily attached to participant's telephone and telephone outlet. If participant does not have a phone line, list your available options to provide cellular reporting. The total cost for RF service via landline and via cellular is to be listed on Price Sheets. Vendor shall provide toll free telephone lines for reporting purposes.	**Sentinel exceeds this requirement.** Sentinel recognizes the growing trend of offenders to do away with landline home phone lines. To directly address this need, Sentinel is pleased to propose the most secure radio frequency models offered in the industry, including **RF Patrol® Landline** and **RF Patrol® Cellular**. Sentinel is pleased to offer two (2) models of **RF Patrol®** receiver/monitor units. The **RF Patrol® Landline** PHMU communicates all reports to the monitoring center via a landline communications network. Sentinel also offers an **RF Patrol® Cellular** PHMU that communicates all reports to the monitoring center via the wireless communications network. Both the **RF Patrol® Landline and Cellular** PHMUs are programmed remotely to report over toll-free telephone numbers. The **RF Patrol® Landline** PHMU is installed in a central location, using a standard two-prong 110 volt AC power cord certified to UL standards and two (2) standard, universal RJ11C connectors that are common in participant homes. It is virtually impossible to connect the unit incorrectly, as installers can connect either RJ11C connector to the wall phone jack or the telephone. The **RF Patrol® Landline** PHMU uses common telephone lines using rotary, pulse, touch tone, broadband, DSL and VoIP telephone systems to transmit data to the monitoring center. If the participant does not have a residential telephone line, **Sentinel offers RF Patrol® Cellular** at an additional cost. The **RF Patrol® Cellular** units utilize the same transmitters and have all of the advanced features as the landline units. The **RF Patrol® Cellular** PHMU incorporates a cellular modem for reporting information to the monitoring center in lieu of using a conventional land-based phone line. **IMPORTANT SENTINEL ADVANTAGE: The RF Patrol® Cellular** unit is one "integrated unit," meaning that the PHMU receiver and cellular unit is an all-in-one "integrated" device requiring only a power cord for installation. Both **RF Patrol®** units incorporate an industry-leading intelligent movement sensor known as "tilt detection" built-in that can aid the officer in differentiating between momentary movement and attempted relocation of the unit. The **RF Patrol® Cellular** unit is superior to competitor products because it was

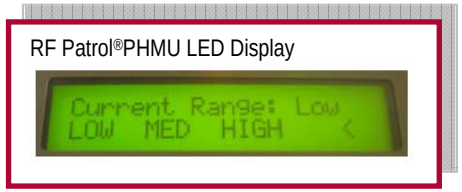
			designed specifically for electronic monitoring. It is not a modified cell phone requiring a secondary device cabled to the unit for communication. This Sentinel technological advantage eliminates the need for additional device inventory and lowers the overall cost of cellular radio frequency monitoring as it utilizes fewer devices. Additionally, Sentinel's **RF Patrol® Cellular** guarantees longer operating battery charge as it is not limited by a traditional cell phone battery. Sentinel has provided the total cost for RF service via landline and via cellular on the Price Sheets as required and all Sentinel proposed devices utilize toll free telephone lines for reporting purposes.
8.22	Receiver	Each receiver shall be capable of simultaneously monitoring multiple transmitters, each with its own unique curfew schedule. Describe this capability including the number of transmitters each receiver can monitor. Also describe the specific steps necessary for an Officer to assign each transmitter to the receiver.	**Sentinel meets this requirement.** Any RF Patrol® PHMU can be programmed to **simultaneously recognize and report statuses from up to 50 PTX2s on one (1) PHMU,** each with its own unique curfew schedule including multiple participants in the same home or guest transmitters in the vicinity of the PHMU. Should an officer choose to the assign multiple transmitters to any one (1) PHMU, he and/or she will follow these steps: Enrolling multiple PTX2s to a single PHMU: ▪ The PHMU will scan for any PTX2s within range ▪ A PTX2 serial number will appear on the LCD display ▪ Select ACEPT & Select IGNR to bypass other units  ▪ Attach the transceiver to the participant's ankle with LED Facing upwards ▪ The PHMU will confirm the band is properly installed on the participant with green flashes. If red, refit band. ▪ The PHMU will then offer the opportunity to enroll more PTX2s. ▪ If there are more PTX2s to be enrolled, select **YES** and the PHMU will return to the activation step to repeat the enrollment process. If no other enrollments are required, select **NO**.

8.23	Receiver	The Receiver shall have FCC approval for home use. Proposals must include the FCC approval number.	**Sentinel meets this requirement.** All of the proposed equipment complies with all appropriate FCC regulations. Sentinel has provided the receiver FCC Identifier Numbers below and copies of all the RF Patrol® certifications are included in the Exhibits section of this proposal: **Part 15** ▪ RF Patrol® PHMU Landline NSNPHMUL08 ▪ RF Patrol® PHMU Cellular NSNPHMUC08 **Part 68** ▪ RF Patrol® US:YEVMM06BPHMUL08
8.24	Receiver	In the event of power disconnect or commercial outage the receiver shall 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.	**Sentinel exceeds this requirement.** The **RF Patrol® Landline** PHMU is powered using a standard two-prong 110 volt AC power cord certified to UL standards. The **RF Patrol®** PHMU is designed with a built-in auto-recharging backup battery that functions for up to 48 continuous hours of full operation (including but not limited to detecting and reporting information) in the event of a commercial power failure at the participant's home or power cord disconnection. Additionally, the PHMU will produce a red front panel indicator light to encourage the participant or other person in the home to ensure the unit is properly plugged in and to reconnect the PHMU power cable if he or she discovers a problem. Despite the reason for power outage, the built-in back-up battery will provide full operation (including dialing and reporting) during continuous power outages for up to 48 hours. Receivers of some other manufacturers do not offer complete operation until 110 volt AC power is restored, dramatically impacting response times for notification. This feature is particularly important to agencies that do not have weekend and/or holiday officer coverage to respond to exceptions. Sentinel can notify the agency immediately each time there is a power outage or restoration of power. **IMPORTANT SENTINEL ADVANTAGE:** In the unlikely event that a power outage exceeds the 48 hour battery back-up and is forced to shut down prior to reporting any event, the **RF Patrol®** PHMU has an internal non-volatile memory capable of indefinitely storing 1024 events (over 90 days of events), including date and time stamps. The unit retains all stored events and reports them to the monitoring center upon power restoration.

8.25	Receiver	System must offer a secure means for the Officer to simply and rapidly perform a range test to confirm signal coverage between the transmitter and receiver in the participant's home. Describe the steps involved for an Officer to conduct a range test, including but not limited to steps involved, whether or not there is a need for monitoring center involvement, indications of signal reception and time required.	**Sentinel meets this requirement.** Sentinel offers the agency added confidence that its participants are reliably monitored while in their residences. **RF Patrol®** was specifically designed to provide the officer with secure direct control of the device, including but not limited to the ability to conduct range testing, **without** the need for monitoring center involvement. Sentinel **RF Patrol®** equipment offers a unique feature that allows for visual range testing during the installation process. While installing the PHMU in the participant's residence, installers have the capability to test the range between the PTX2 and the PHMU to ensure the agency will not receive false out-of-range alarms when the participant is inside their residence. This capability also assists the installers through ensuring that the range setting between the PTX2 and the PHMU is small enough to securely confine the participant to his or her home during curfew hours.

			Performing a Range Test: ▪ Turn the PHMU Menu Key to the horizontal position ▪ Select RNG (range) from the Setup Menu ▪ Select TEST from the RNG Menu ▪ The LCD screen will display the words "Testing" and a negative (-) sign to the upper left and a positive (+) sign to the right of the LCD screen. ▪ The transmitter will immediately begin to blink ▪ One (1) blink from the PTX2 indicates excellent range, two (2) blinks indicates good range, three (3) blinks indicate poor signal reception and four (4) blinks indicate no signal reception (no longer in range) ▪ Installer may walk with the participant to each section of the home during the range test to confirm range PTX2 LED Light PHMU Signal Strength and LED Lights

			▪ Once all areas of the home have been covered, select the [<] less than symbol to end the range test and return to the main menu ▪ Once the range test ends, the PTX2 will stop blinking 
8.26	Receiver	The Receiver shall record and report a tamper signal if the case is opened.	**Sentinel meets this requirement.** The **RF Patrol®** PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect **and all attempts to open the receiver case/housing**. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU. In addition to PHMU tampers, the unit will detect and communicate all other alerts and notifications, including but not limited to PTX2 tampers, arrival

			and departures of the PTX2, loss and restoration of power or telephone service, and HMU Overdue.
8.27	Receiver	System must be capable of varying the signal range between transmitter and receiver for each device to best match the risk of each participant and the signaling coverage in each participant's home. Identify the number of settings and general distances of the available range settings of your proposed RF system.	**Sentinel meets this requirement.** During set-up the **RF Patrol®** monitoring system's **signal range (range between the PTX2 and PHMU) is agency programmable and variable with three (3) settings** as follows: ▪ Low, approximately 50 feet ▪ Medium, approximately 100 feet ▪ High, approximately 150 feet **RF Patrol®** was specifically designed to provide the officer with secure direct control of the device, including but not limited to the ability to change range settings and/or conduct range testing, **without** the need for monitoring center involvement. Sentinel **RF Patrol®** equipment offers **a unique feature that allows for visual range testing during the installation process**. While installing the PHMU in the participant's residence, installers have the capability to test the range between the PTX2 and the PHMU to ensure the agency will not receive false out-of-range alarms when the participant is inside their residence. This capability also assists the installers through ensuring that the range setting between the PTX2 and the PHMU is small enough to securely confine the participant to his or her home during curfew hours. 
8.28	Receiver	The Receiver shall perform internal diagnostics to determine if it is operating properly. These diagnostics shall be reported by the Receiver to the Monitoring Center computer and displayed in the event history.	**Sentinel exceeds this requirement.** While in setup mode, officers can quickly view settings through the front panel display and configure or change settings using the front panel keypad. Upon initial activation, the **RF Patrol®** PHMU unit's front LCD panel displays visible written confirmation that the PTX2 band is securely closed and a visual signal strength indicator. Additionally, Light-Emitting Diode (LED) lights on the PHMU provide a clear indication that it is receiving the signal from the transmitter.

Sentinel' **RF Patrol®** PHMU provides both LED lights and an LCD display to ensure full functionality and to display power statuses, RF signal strength and many other operational messages. **RF Patrol®** PHMU features three (3) LED lights directly above the LCD screen that illuminate under the following conditions:

- The red light on the left is associated with PHMU calling in events
- The yellow light in the middle is associated with the phone line connection
- The green light on the right is associated with the power connection

PHMU Signal Strength and LED Lights

Additionally, to confirm proper operation and telephone connectivity, the PHMU will report at least once every four (4) hours to the monitoring center. **On average, an RF Patrol® PHMU will communicate with the monitoring center approximately 10 to 20 times a day.** The Sentinel monitoring center does not need to call the PHMU or ring the participant's home telephone to verify operation and location. Instead, **RF Patrol®** silently verifies proper operation by implementing regularly scheduled calls from the PHMU to the central computer, using an internal timer unique for each PHMU enrolled. If the PHMU does not report to the monitoring center after four (4) hours, the PHMU generates an **"HMU Overdue"** notification signifying that the PHMU cannot or has not been able to report at its regular interval. The duration of the reporting interval is programmable in one-hour increments and remotely programmable by the monitoring center via remote access with the PHMU, without the need to go to the participant's home.

Additionally, the RF Patrol® receiver will report the following events to the monitoring center computer. These events will be displayed in the event history and additionally, Sentinel can provide alert notifications based on agency-specified notification profiles for a wide array operating malfunctions and internal diagnostics both during monitoring initialization and routine operation of the equipment. During initial activation:

Notification Exceptions	Description
Remote PTX2 Add	A PTX2 has been enrolled to the PHMU remotely.
Officer PID Detected	The PHMU has detected an OPID in its range.
Officer PID Disappeared	The PHMU is no longer detecting an OPID in its range.
Invalid Officer PID Detected	The PHMU has detected an invalid OPID in its range.
Officer PID Out Of Sync	The OPID and PHMU may be out of sync. Repeat occurrences require further investigation.
PHMU In Officer Mode	The PHMU Menu Key has been turned to the Setup Mode.
PHMU In Monitoring Mode	The PHMU Menu Key has been turned to the Monitoring Mode.
Key To Menu Mode	The PHMU Menu Key has been turned to the Setup Mode.
Key to Officer Mode	The PHMU Menu Key has been turned to the Monitoring Mode.
HMU Enrollment	The enrollment process of the RF Equipment has begun.
HMU Installation Complete	The installation process of the RF Equipment is complete.

During monitoring:

Notification Exceptions	Description
HMU Diagnostics	The PHMU has provided internal operating and diagnostic information.
HMU System Source	The PHMU has provided internal operating and diagnostic information.
Out of Sync.	The PTX2 and PHMU may be out of sync. Repeat occurrences may require further investigation.
Remote PTX2 Change	The PTX2 being monitored has been changed remotely.
Remote PTX2 Remove	A PTX2 has been removed from the PHMU remotely.
Foreign PTX2 Detected	The PHMU has detected a foreign PTX2 in its range.
Foreign PTX2 Disappeared	The PHMU is no longer detecting a foreign PTX2 in its range.

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Foreign PTX2 Detected</td><td>The PHMU has detected a foreign PTX2 in its range.</td></tr>
<tr><td>Foreign PTX2 Disappeared</td><td>The PHMU is no longer detecting a foreign PTX2 in its range.</td></tr>
</table>
</td></tr>
<tr><td>8.29</td><td>Receiver</td><td>The Receiver shall continually attempt to dial into the Monitoring Center until it makes contact and downloads data or until power is disconnected or battery depleted.</td><td>
Sentinel meets this requirement. During communication outages, Sentinel' RF Patrol® units will continue to monitor the participant and store data in its internal non-volatile memory with the capability to store 1024 events (over 90 days of events) with date and time stamps of occurrence. The units will continually attempt to dial into the monitoring center until it makes contact and downloads data or until power is disconnected or battery depleted. The unit will report all stored data to the monitoring center upon restoration of communications.
IMPORTANT SENTINEL ADVANTAGE: As the following table indicates, Sentinel' RF Patrol® provides agencies added confidence that a participant is monitored even during commercial power or telephone outages. Through offering expanded non-volatile memory capabilities and 48 hours of battery back-up power, Sentinel provides the agency sufficient time to investigate the source of the outage once it receives notification from Sentinel of a power or telephone disconnect and take the necessary precautions to ensure public safety is maintained.
<table>
<tr><th colspan="3">RF Patrol® Back-up and Storage Capabilities during Outages</th></tr>
<tr><th>Power</th><th>Communication</th><th>Sentinel Solution To Address Outage</th></tr>
<tr><td>X</td><td></td><td>RF Patrol® units provide for 48 hours of full continuous operation in the event of a power outage. The units will continue to report all alerts and events to the monitoring center during this 48 hour period.</td></tr>
<tr><td></td><td>X</td><td>Sentinel' RF Patrol® units will continue to monitor the participant and store data in its internal non-volatile memory with the capability to store 1024 events (over 90 days of events). The units will report all stored data to the monitoring center upon restoration of communications.</td></tr>
</table>
</td></tr>
</table>

				X	Sentinel' **RF Patrol®** units will continue to monitor the participant and store data in its internal non-volatile memory with the capability to store 1024 events (over 90 days of events). The units will report all stored data to the monitoring center upon restoration of communications.
			X	X	Sentinel' **RF Patrol®** units will operate on the 48 hour battery back-up and store information in the internal non-volatile memory with the capability to store 1024 events (over 90 days of events). The units will report all stored data to the monitoring center upon restoration of communications.
8.30	Receiver	A Leave Window count-down timer exists within all RF Receivers as a means of preventing false "Leave" events during short term signal loss while the transmitter is still in range. This Leave Window must be adjustable at the Agency's direction on a per unit/participant basis.	**Sentinel meets this requirement. RF Patrol® features a programmable leave window** at the participation agency's direction either all units shipped to an agency or on a per unit/participant basis. The standard leave window is five (5) minutes, but can easily and remotely be adjusted. **IMPORTANT SENTINEL ADVANTAGE: RF Patrol®** has one of the shortest standard departure "leave windows" in the industry with a default five-minute leave window without producing false leave signals, allowing **RF Patrol®** to report departures and arrivals faster and more accurately that any other vendor on the market. This is achievable due to **RF Patrol®'s Dual Transceiver, Two-way RF Link Approach.** Sentinel' unique dual transceiver approach incorporates both a transmitter and receiver in the PHMU, as well as having both in the PTX2. In fact, the **RF Patrol®** PHMU has two (2) constantly active internal antennas capable of both receiving from and transmitting signals to the PTX2 to maximize the ability to detect the presence of transmitter signals. For the first time in the industry, the two (2) components truly communicate with each other, automatically confirming alerts in advance of reporting.			
8.31	Receiver	A Reporting Window count-down timer exists within all RF systems as a means of regularly confirming that the Receiver is connected to the phone line and capable of reporting events (not disconnected from the phone line and unable to report, such as	**Sentinel meets this requirement. The duration of the PHMU reporting window is adjustable in one-hour increments and remotely adjustable. The setting can be configured for either all units shipped to an agency or on a per unit/participant basis.** The default is PHMU leave window will report at least once every four (4) hours to the monitoring center to confirm proper operation and telephone connectivity. On average, an RF Patrol® PHMU will		

<table>
<tr><td></td><td></td><td>disconnected by a participant before leaving range). This Reporting Window must be adjustable at the Agency's direction on a per unit/participant basis.</td><td>communicate with the monitoring center approximately 10 to 20 times a day. The Sentinel monitoring center does not need to call the PHMU or ring the participant's home telephone to verify operation and location. Instead, RF Patrol® silently verifies proper operation by implementing regularly scheduled calls from the PHMU to the central computer, using an internal timer unique for each PHMU enrolled. If the PHMU does not report to the monitoring center after four (4) hours plus a one (1) hours grace period , the PHMU generates an "HMU Overdue" notification signifying that the PHMU cannot or has not been able to report to the monitoring center at its regular interval.</td></tr>
<tr><td>8.32</td><td>Receiver</td><td>The Receiver shall detect and report events related to disconnect and reconnect of the electrical power and telephone line.</td><td>Sentinel meets this requirement. Each RF Patrol® PHMU detects and reports events related to disconnect and reconnect of the electrical power and telephone line. Additionally, Sentinel provides alert notifications for a wide array of loss and/or restoration of telecommunications events including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>Telephone Disconnect</td><td>The telephone line has been disconnected from the PHMU.</td></tr>
<tr><td>Telephone Reconnect</td><td>The telephone line has been connected to the PHMU.</td></tr>
<tr><td>Communication Circuits Busy</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to busy circuits.</td></tr>
<tr><td>Communication No Answer</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to no answer.</td></tr>
<tr><td>Communication Break</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to call interruption.</td></tr>
<tr><td>Communication No Dial Tone</td><td>The PHMU has experienced temporary difficulty with landline telephone communications due to no dial tone.</td></tr>
</table>
Sentinel also provides alert notifications for the loss and/or restoration of alternating current (AC) power events including:
<table>
<tr><th>Notification Exceptions</th><th>Description</th></tr>
<tr><td>Power Disconnect</td><td>The electrical power supply has been disconnected from the PHMU.</td></tr>
</table></td></tr>
</table>

			Power Reconnect — The electrical power supply has been connected to the PHMU. **PHMU Forced Power Down** — The PHMU has been manually powered down. **HMU Power Up** — The PHMU has been powered up.
8.33	Receiver	The Receiver should detect and report movement and be able to differentiate momentary (such as cleaning around the Receiver) versus perpetual movement (such as relocation).	**Sentinel meets this requirement.** Both **RF Patrol®** units (landline and cellular) incorporate an industry-leading **intelligent movement sensor known as "tilt detection"** built-in that can aid the officer in differentiating between momentary movement and attempted relocation of the unit. The will report an "HMU Tilt" event when the PHMU has been continually moved for approximately 20 seconds or longer and the "HMU Tilt" event can repeat providing the capability to differentiate momentary (such as cleaning around the receiver) versus perpetual movement (such as relocation).
8.34	Receiver	The Receiver should incorporate at least a 1000 event non-volatile memory to store events (with date and time of occurrence) at times when the phone line is not available and continually attempt to report them until reporting has been successful.	**Sentinel meets this requirement.** During communication outages, Sentinel' **RF Patrol®** units will continue to monitor the participant and store data in its internal non-volatile memory with the capability to store 1024 events (over 90 days of events) with date and time stamps of occurrence. The units will continually attempt to dial and report into the monitoring center until it makes contact and downloads data or until power is disconnected or battery depleted. The unit will report all stored data to the monitoring center upon restoration of communications.
8.35	Receiver	The Receiver must allow use with any brand or make of telephone line including touch tone, broadband, and DSL and VoIP.	**Sentinel meets this requirement.** The **RF Patrol® Landline** PHMU uses most any common brand or make of telephone lines using rotary, pulse, touch tone, broadband, DSL and VoIP telephone systems to transmit data to the monitoring center.
8.36	Receiver	The Receiver shall 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 shall have the ability to record the actual time of occurrence.	**Sentinel meets this requirement.** The **RF Patrol®** PHMU will detect and communicate all participant status changes including but not limited to PTX2/PHMU tampers, arrival and departures of the PTX2, loss and restoration of power or telephone service, other internal diagnostics, and HMU Overdues. All participant status changes will be recorded and reported by the PHMU to the monitoring system with the actual date and time of occurrence. Additionally, the monitoring system computer will record the date and time of receipt of each event report.

8.37	Receiver	The Receiver shall 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.	**Sentinel meets this requirement.** The **RF Patrol®** PHMU will detect and communicate all participant status changes 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. On average, an RF Patrol® PHMU will communicate with the monitoring center approximately 10 to 20 times a day.
8.38	Receiver	The Receiver shall 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 shall be time and date stamped with actual time of occurrence.	**Sentinel meets this requirement.** The **RF Patrol®** PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. If telephone service is interrupted, the PHMU will prioritize and store activity data in the PHMU non-volatile internal memory, automatically reporting the statuses **immediately** (within one (1) minute) upon the restoration of telephone service. All participant status changes will be recorded and reported by the PHMU to the monitoring system with the actual date and time of occurrence. Additionally, the monitoring system computer will record the date and time of receipt of each report.
9.0	**SECTION I Equipment**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
9.1	Equipment Inventory/Supplies	Deleted	
9.2	Equipment Inventory/Supplies	At no additional cost to the Agency the Vendor shall supply replacements for lost, stolen and damaged equipment equal to five (5%) percent of the Agency's active units for offenders on an annualized basis. Detail cost to agency of each piece of equipment should payment be required.	**Sentinel meets this requirement.** At no additional cost to the agency, Sentinel will supply replacements for lost, stolen and damaged equipment equal to five percent (5%) of the agency's active units for offenders on an annualized basis. Sentinel has provided the per-component cost for lost, stolen or damaged replacement equipment in excess of the annualized 5% allowance in the pricing section of this proposal should payment be required.

9.3	Equipment Inventory/Supplies	The Vendor shall provide and maintain a backup/replacement inventory of monitoring units up to fifteen percent (15%) of the actual number of units in use with Agency under this contract at no additional cost. The Agency shall not pay the Vendor an inventory fee, storage fee, installation equipment fee or another fee related to inventory units and equipment. The Agency shall only be obligated to pay the per-day activated unit rate as set forth in the Contract.	**Sentinel meets this requirement.** Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and available as **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. Sentinel understands that no agency will be required to pay an inventory fee, storage fee, installation equipment fee or another fee related to inventory units and equipment. Sentinel acknowledges that participating agencies shall only pay the per-day activated unit rate as set forth in the Contract.
9.4	Equipment Inventory/Supplies	The Vendor shall ship equipment within three (3) business days or, if spare inventory has been depleted, within 24 hours of receipt of order. In the event any equipment becomes inoperative due to a malfunction or through normal use, the Vendor shall incur all replacement costs and repairs. The Vendor shall provide the Agency with replacement equipment within five (5) business days or, if spare inventory has been depleted, within 24 hours of receipt of order. The Vendor shall pay all costs associated with shipping (both delivery and return) of all equipment and supplies.	**Sentinel meets this requirement.** Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including **RF Patrol®** and confirms that all equipment provided to each Western States Contracting Alliance participating agency is covered by a full manufacturer's warranty **for the length of the contract**. Sentinel will maintain all equipment in good operating condition and free from materials defects and/or workmanship under normal and proper use for the term of this agreement. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. Sentinel's assigned Account Manager will work proactively with each Western States Contracting Alliance participating agency to ensure the appropriate amount of equipment and spares are maintained for the electronic monitoring of offenders. This open communication aids Sentinel in assuring ample equipment is available to meet each agency's needs Sentinel will ship all initial and new equipment orders within three (3) business days. Additionally, if any agency's spare inventory is depleted, Sentinel will re-supply the appropriate equipment via overnight delivery at no additional cost within 24 hours after notification.

			In the event of any malfunction of any piece of equipment, Sentinel will provide routine equipment maintenance repair through the return and replacement of malfunctioning equipment at no additional cost to participating agencies. Sentinel will ship all replacement equipment within five (5) business days. All shipping costs (both delivery and return) of all equipment and supplies will be the responsibility of Sentinel.
10.0	**CATEGORY 1 – RADIO FREQUENCY (RF) RANDOM/SCHEDULED TRACKING SERVICE**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
10.1	Random Tracking	The tracking system should provide random location verification of the participant in multiple locations such as home, work, school, and treatment by a telephone or alert device.	**Sentinel exceeds this requirement.** The electronic monitoring solution detailed in this proposal is the latest voice verification technology available on the market and will serve to provide the best value, as well as help ensure public safety and maintain participant confidentiality. Sentinel is offering newer, more state-of-the-art technology in proven use nationally and has highlighted throughout this proposal areas where Sentinel can provide an advantage over other electronic monitoring providers. For minimum risk participants, Sentinel proposes **Voice Patrol®**, an innovative and effective voice verification solution to meet step-down or reduced supervision needs. The **Voice Patrol®** system is an electronic monitoring program that uses voice verification technology, the Public Switched Telephone Network and a standard telephone to verify the presence of an individual at a specified location or multiple locations such as home, work, school, and treatment. The following list highlights some of the unique features of the **Voice Patrol®** solution: ▪ **Accurate Identification:** Identifies imposters 99.2% of the time, distinguishes between identical twins and positively verify participants with a cold. ▪ **Multiple Monitoring Methods:** Allows agencies to select and edit scheduled, random or on-demand verifications on a per participant basis. ▪ **Smart System Technology:** Improves the quality of each participant's voice template with each successful verification call providing increased verification accuracy throughout a participant's term of monitoring. ▪ **Multiple Languages Capability:** Ability to monitor participants in multiple different languages including English and Spanish.

			▪ **Supports Calls In and Out of the System:** Supports both inbound and outbound verification calls which can accommodate a variety of schedules and time windows. ▪ **No Busy Signals:** Access to multiple authorized call-in phone numbers from Sentinel's established bank of verification phone lines or allows agencies to request a dedicated line(s) for its participant population. ▪ **Customized Monitoring:** Supports the delivery of customized voice announcements, messages and prompts specific to agency's needs on a per participant basis including the ability to require either a numeric response or voice response from the participant. ▪ **Message Capability:** Capability for participants to leave messages within the verification system for playback via web browser. ▪ **Web-based Interface:** Fully integrated monitoring in Sentinel's web-based information exchange, SenTrak.
10.2	Random Tracking	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:	**Sentinel meets this requirement. Voice Patrol®** provides the latest technology, utilizing a computer to generate scheduled, random or on-demand calls during specified time periods while at home or away from home. The computer can also receive calls to and from participants and confirm whether the participant is at authorized/required locations during specific time periods.
10.3	Random Tracking	a. Accurately verifying the presence of the participant/unit.	**Sentinel exceeds this requirement.** The **Voice Patrol®** system has the capability to accurately verify both the location of the participant during verification calls and positively identify the identity of the participant. On all incoming calls, the Automated Number Identification (ANI) of the originating phone number is validated against a list of approved authorized locations in addition to the verification of the individuals' identity. By combining these two (2) calling processes, the **Voice Patrol®** system has the ability to monitor and track individuals throughout the day, even though they may be authorized to leave their permanent residence. **IMPORTANT SENTINEL ADVANTAGE: Voice Patrol®** identifies imposters with an exceptional level of accuracy. This technology incorporates several advanced design features that significantly enhance system reliability and performance including the ability to extract the voice recording from line noise, so telephone types and line quality are more flexible then in earlier generation voice verification systems.

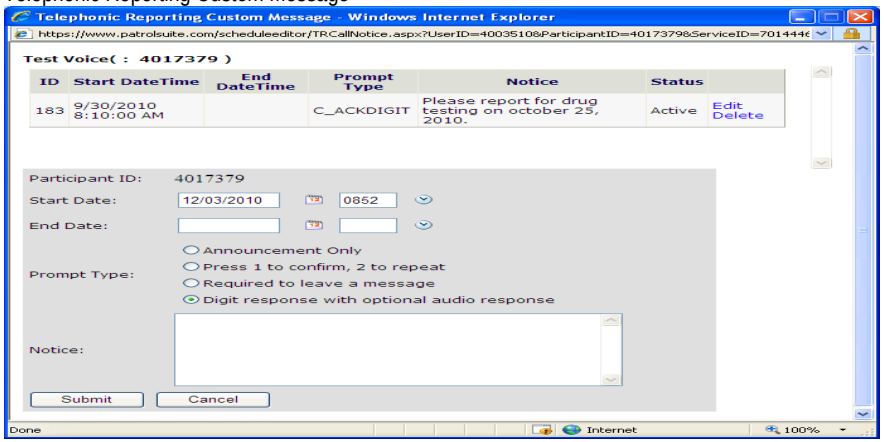
10.4	Random Tracking	b. Confirming the location/phone number of the participant/unit.	**Sentinel meets this requirement.** During outbound calls, the **Voice Patrol®** system will automatically call the appropriate telephone number corresponding with the participant's required location during a specified date and time. On all incoming calls, the Automated Number Identification (ANI) of the originating phone number is validated in addition to verification of the individuals' identity. The system will then automatically verify that the participant is calling from a pre-authorized location consistent with the specific date and time of the call. By combining these two (2) calling processes, the **Voice Patrol®** system has the ability to monitor and track individuals throughout the day, even though they may be authorized to leave their permanent residence.
10.5	Random Tracking	c. Verifying the time of the random/schedule event.	**Sentinel meets this requirement.** During outbound calls, the **Voice Patrol®** system will automatically call the appropriate telephone number corresponding with the participant's required location during a specified date and time. On all incoming calls, the system will automatically verify that the participant is calling from a pre-authorized location consistent with the specific date and time of the call.
10.6	Random Tracking	d. Performing both random and scheduled contacts at predetermined locations and times.	**Sentinel meets this requirement. Voice Patrol®** provides the latest technology, utilizing a computer to generate scheduled, random or on-demand calls during specified time periods while at home or away from home. The system has the capability to accept inbound calls from multiple locations and automatically compare the Automated Number Identification (ANI) of the originating phone number as verification against the numbers of predetermined locations stored in memory. This provides capability of verification of predetermined locations.
10.7	Random Tracking	The average number of tracking contacts (for both Random and Scheduled) shall be five (5) contacts per participant per day. The actual number utilized post-award may vary per participant depending on the level of supervision required. The unit/day pricing for tracking shall be inclusive of, but not limited to: all participant enrollment, tracking contacts, data changes, and participant termination. One (1) completed contact shall collectively include all of the following:	**Sentinel exceeds this requirement.** Based on the call schedules entered during the pre-enrollment process, the **Voice Patrol®** system generates random and scheduled verification calls to the enrollee's monitoring locations on the average of five (5) times per participant per day. **IMPORTANT SENTINEL ADVANTAGE:** When placing random verification calls, **Voice Patrol®** features a unique statistical algorithm to distribute an agency defined average number of calls per curfew period in a truly random manner to make the prediction of calls unfeasible for a participant. **Please note** that the agency will only define a average number of calls, for example if a customer sets an average number of calls of five (5) per day, the participant may receive four (4) calls on any given day, five (5) calls on any given day or three (3) calls on any given day making it truly impossible for a participant to determine if he or she will be receiving additional calls or not during his or her curfew period.

			The verification calls are randomly distributed throughout the calling period based on the length of the calling period and the number of calls to be placed. Optionally, a verification call can be placed at the beginning and/or end of a call schedule (for curfew monitoring) with the remainder of the calls distributed throughout the calling period. In addition to the random calls automatically generated by the system, scheduled verification calls can be manually added for a specific time using the call maintenance facility incorporated into the web-based monitoring platform. Sentinel confirms the per day pricing for Voice Patrol® provided in the pricing section of this proposal is inclusive of, but not limited to: all participant enrollment, tracking contacts, data changes, and participant termination.
10.8	Random Tracking	a. Any Vendor activity required generating a participant alarm soliciting the participant to report.	**Sentinel meets this requirement.** Sentinel confirms that one (1) completed contact shall collectively include all events in this requirement and any Sentinel activity required generating a participant alarm soliciting the participant to report. Based on the call schedules entered during the pre-enrollment process, the **Voice Patrol®** system generates random and scheduled verification calls to the
10.8	(Continued)		enrollee's monitoring locations to solicit the participant to perform a location verification. When a verification call is placed and answered, the system will play a brief welcome message and then instruct the answering party to "press any key to continue". The system will then prompt the enrollee to repeat two (2) paired number sequences called digit sets. Following the final response, the system will inform the enrollee that the verification session is completed. Verification sessions take approximately 15 seconds to complete. **IMPORTANT SENTINEL ADVANTAGE:** Each verification session includes a 'Liveness' test. The **Voice Patrol®** system features the ability to randomly select one (1) of three possible digit sets therefore making it impossible for the participant to predict the required digit set and pre-record a verification.
10.9	Random Tracking	b. Participant's response to the alarm to confirm compliance.	**Sentinel meets this requirement.** Sentinel confirms that one (1) completed contact shall collectively include all events in this requirement and participant's response to the alarm to confirm compliance. **Voice Patrol®** records and stores participant voice responses and also allows authorized users to listen to the verification sections and any optional voice messages left by participants through Sentinel's SenTrak, an advanced web-based information exchange platform. **Customized Messages:** Through the SenTrak software, the system has the ability to add customized messages and prompts on a per participant basis

during any scheduled, random or on-demand verification call. A unique feature of the customized messages and prompts capability includes the ability to define the level of interaction with the participants including defining the messages as:

- ✓ Announcement Only: The participant will receive a voice reading of a typed announcement during his or her next call.
- ✓ Require Response (Press 1 to confirm, press 2 to repeat): The participant will receive a voice reading of the typed message and then be prompted to confirm receipt of the message.
- ✓ Required To Leave a Message: The participant will receive the typed message as a voice question and be required to record a voice response.
- ✓ Digit Response with Optional Audio Response (Press 1 to confirm, press 2 to leave message): The participant will receive a voice reading of the typed message and then be prompted to confirm receipt of the message or optionally to record a voice response.

Telephonic Reporting Custom Message



10.10	Random Tracking	c. The exchange of tracking information (including enrollment, data changes, monitoring/tracking reports and terminations) between the Officers and the Vendors Monitoring Center shall occur via secure, real-time access by using Agency's existing computer/internet access.	**Sentinel exceeds this requirement.** Sentinel confirms that one (1) completed contact shall collectively include all events in this requirement and the exchange of tracking information (including enrollment, data changes, monitoring/tracking reports and terminations) between the officers and the monitoring center shall occur via secure, real-time access by using agency's existing computer/Internet access. SenTrak, Sentinel's advanced Internet information exchange platform, functions fully with Sentinel's **Voice Patrol®** equipment. **Sentinel's internal IT department developed, owns and operates the SenTrak system, providing in-house maintenance expertise as well as total control over the database, data field queries, reports and overall operations.** SenTrak software uses leading Internet security features, including 128-bit encryption and Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **Sentinel customers do not need to purchase or download any custom hardware or software.** Upon program enrollment, Sentinel assigns security passwords and unique login names to each agency authorized user. SenTrak allows all authorized users and monitoring personnel with a computer and Internet browser (i.e. home computer, office computer, other) to exchange monitoring and tracking data, computer, office computer, other) to exchange monitoring and tracking data, such as enrollment, verification schedules, curfew changes, caseload review, notifications, reports and terminations, with the Sentinel monitoring center using secure website access. **Web-Based Enrollment:** The computer system immediately and automatically stores all of the data entered at the time of enrollment. This feature provides a quick efficient and accurate method for entering data into the monitoring system. SenTrak date and time stamps, and records the user login name for all remote data entries. If a user in the field opts to call information into the monitoring center, monitoring center staff will enter the information and store the entries with a date and time stamp and the name of the monitoring center associate. SenTrak has proven to increase efficiency, reduce data entry time, increase accuracy, and provides the most cost effective and virtually paperless solution to Sentinel clients.

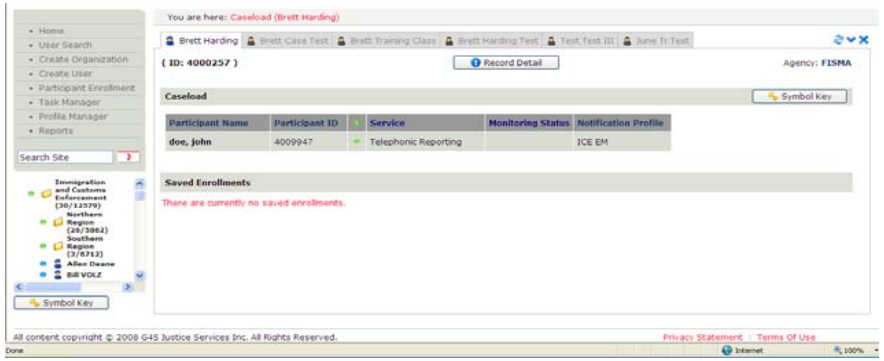
Enrollment information includes relevant personal information for each participant, including but not limited to name, address and telephone number(s). To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's name, relevant addresses and phone numbers, supervising agency and officer information, along with monitoring service type. Please note that the SenTrak system allows agencies to request customized fields for additional agency specific participant information. In addition to entering the basic requirements, an agency can choose participant demographic information it deems necessary and Sentinel will add the agency specific enrollment fields to the Enrollment Screens. Sentinel is the original developer of SenTrak and Sentinel engineers control the web-based data fields, reports and queries, ensuring Sentinel is fully capable of meeting agency data and reporting needs.

Voice Templates: After basic enrollment and scheduling, each participant will be required to record a voice template for comparison for subsequent verification calls. The voice template recording process takes approximately two (2) to three (3) minutes while participants provide three (3) distinct four (4) digit sets of numbers as audio samples. At any time, authorized users can access the SenTrak system to determine if a voice template has been created and also if the creation of a voice template was successful through the following event descriptions:

Description of Event	Event Trigger
Voice Verification Template Not Recorded	Call schedule begins when there is no voice template recorded (no further events generate).
Voice Verification Enrollment Successful	Biometric voice template / VocalPasswords successfully recorded.
Voice Verification Enrollment Failed	Biometric voice template/ VocalPasswords incomplete. Immediately allows officer / participant to call in again.

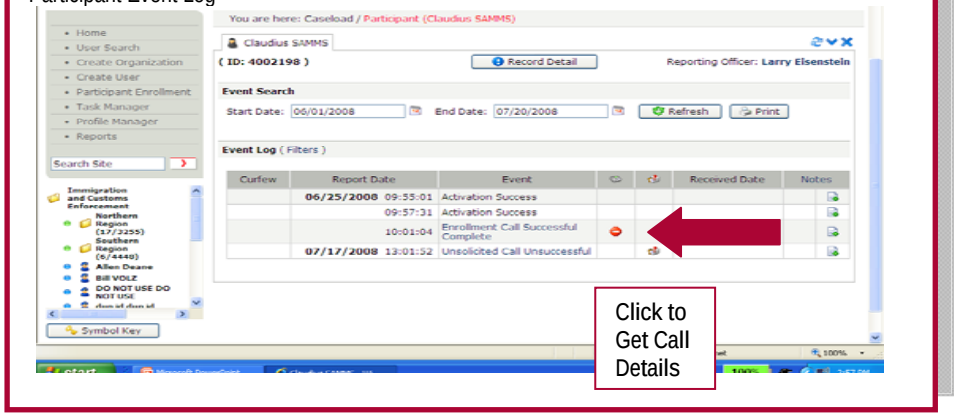
Additionally, at any time during monitoring, Sentinel can reset the participant's voice template upon agency request so the participant can record it again.

Case Load Review: Users also have the ability to directly access participant information through Sentinel's SenTrak. The SenTrak system provides users

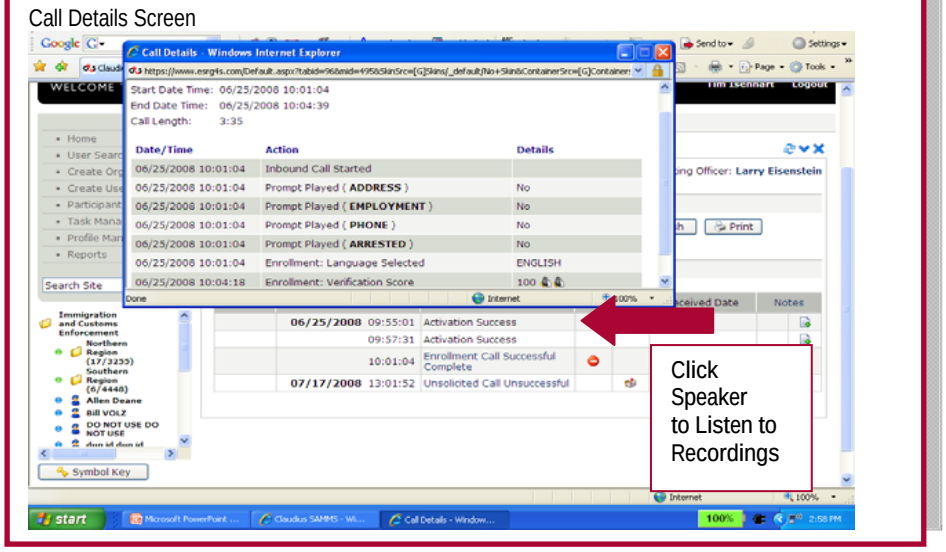
			with real-time access to participant events, daily status and caseload data. Once logged in, any authorized user including agency administrators are able to review their own caseload and participant statuses. The "Caseload Review Screen" lists all participants for a user and utilizes two (2) columns featuring easy to recognize symbols to help users quickly identify a participant's violation status and monitoring statuses. Caseload Review Screen 

Clicking a participant's name in the Caseload Review Screen opens the Event Log screen where a user can view a participant's event log, monitoring statuses or alerts. This Event Log can be limited or expanded through the start date and end date fields. **Additionally through the Event Log, users have the ability to directly access the wave files with the recording on the actually voice verification or to any messages left in the system.**

Participant Event Log

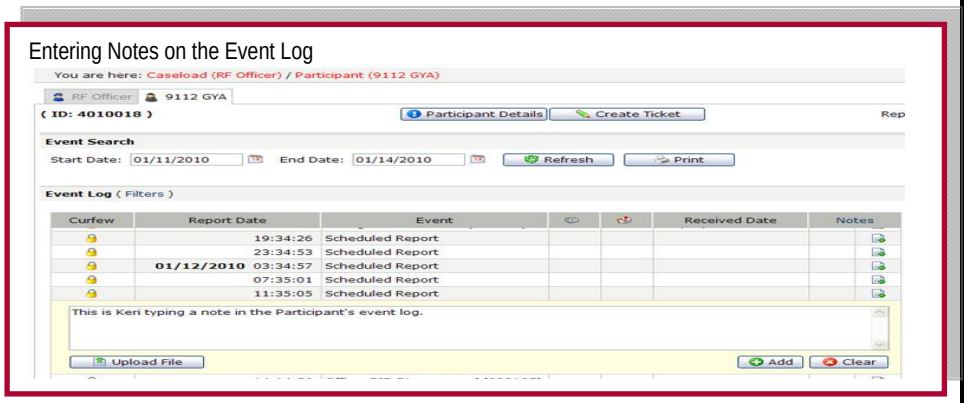


Call Details Screen



Case Notes: Authorized users can enter case notes on a "per participant" or "per event" basis. SenTrak adds the note to the bottom of the screen with a Note in System icon. Once a note has been entered, it cannot be removed from

Case Notes: Authorized users can enter case notes on a "per participant" or "per event" basis. SenTrak adds the note to the bottom of the screen with a Note in System icon. Once a note has been entered, it cannot be removed from the system. All notes are archived to create a clear audit trail of all participant' monitoring activities. The following example shows a case note previously entered by a user. Users can view previously entered case notes by clicking the Note in System icon.



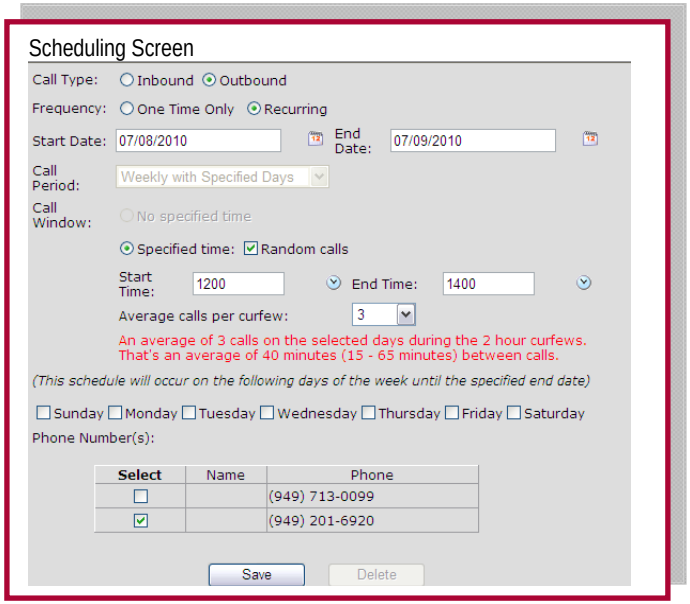
Reports: All monitoring reports are available through the easy-to-use report generator application of Sentinel's SenTrak software. Any authorized user can view participant activity 24 hours a day, seven (7) days a week. Participant activity is posted **in real-time** so users can view violations online as they occur. Sentinel will work with its clients to ensure all needed reports, including on-demand reports, daily and quarterly reports are available.

Through SenTrak Sentinel can provide reports immediately or on an on-going basis addressing the following topics.

- Caseload Management
- Schedules
- Daily Statuses
- Event History
- Alert Notifications
- Billing

If fact, agencies using the **Voice Patrol®** system can choose from **over 15 standard system reports** to help manage their caseloads including two (2) reports which were specifically designed for this product including:

			which were specifically designed for this product including: ▪ Voice Patrol Call Schedules: Provides users with a snapshot of active participants and their current schedules. ▪ Voice Patrol Prompt Response: Provides users with a summary of customer prompt responses from their participants **All reports in SenTrak can be viewed on screen, printed or exported in XML, CSV, TIFF, PDF, HTTP or Excel.**
10.11	Random Tracking	The system should have the ability to randomly contact/alert the participant through a reliable form of notification and must continue to alert the participant until they respond. Conventional pager coverage throughout some areas is inconsistent and unreliable. Therefore, pagers alone are not acceptable for alerting participants. Vendors are to describe in detail their method of contracting/alerting participants.	**Sentinel exceeds this requirement.** **Voice Patrol®** has the ability to randomly contact/alert the participant via telephone calls generated from the SenTrak system to a telephone location for the participant as the method of contracting/alerting participants. Based on the call schedules entered during the pre-enrollment process, the Voice Patrol® system anticipates the receipt of or generates random or scheduled verification call to the enrollee's monitoring location to solicit the participant to perform a location verification. When a scheduled call is not received or answered and/or the voice verification fails, an exception is created and the participant's supervisor is automatically notified by the system. Authorized users may access the exception (alerts) voice message system via SenTrak or telephone. There are six (6) distinct types of failures identified by the **Voice Patrol®** system including a failed voice verification, calling from an unauthorized phone number, missing a scheduled/on-demand outbound call, missing a scheduled/on-demand inbound call, if a participant hangs up after answering or if the line is busy during the scheduled curfew time. **Should any call result in any failure, the system will automatically generate a follow-up verification attempt or retry to the enrollee.** **The numbers of retries that are generated vary by enrollee and are based on the security level that has been assigned by supervising agency. The interval between verification attempts can also vary based on the failure type and is determined by supervising agency.**

10.12	Random Tracking	The tracking system should enable the Officer to set an optional quiet period when no alarms occur. The system should automatically randomize the number of alarms and the times alarms occur from day to day and not require regular Officer grooming of calling schedules.	**Sentinel meets this requirement**. Officers will have to ability to set an optional quiet period by entering both start and stop times for each schedule entered during the pre-enrollment process. The **Voice Patrol®** system will not generate random verification calls to the enrollee's monitoring location during the optional quiet period.  **Voice Patrol®** features a unique statistical algorithm to distribute an agency defined average number of calls per curfew period in a truly random manner to make the prediction of calls unfeasible for a participant. **IMPORTANT SENTINEL ADVANTAGE:** Please note that the agency will only define a average number of calls, for example if a customer sets an average number of calls of five (5) per day, the participant may receive four (4) calls on any given day, five (5) calls on any given day or three (3) calls on any given day making it truly impossible for a participant to determine if he or she will be receiving additional calls or not during his or her curfew period. The verification calls are randomly distributed throughout the calling period based on the length of the calling period and the number of calls to be placed. Optionally, a verification call can be placed at the beginning and/or end of a call schedule (for curfew monitoring) with the remainder of the calls distributed throughout the calling period. In addition to the random calls automatically generated by the system, scheduled verification calls can be manually added for a specific time using the call maintenance facility incorporated into the web-based monitoring platform.

<table>
<tr><td>10.13</td><td>Random Tracking</td><td>The participant should be required to respond to the alert by answering the call from or, calling the toll free number of the Vendor's Monitoring Center. During the participants call, unit/participant identity shall be positively identified to the Monitoring Center by a highly accurate method of positive communication. Vendors are to describe in detail their method of verifying unit/ participant identity.</td><td>Sentinel exceeds this requirement. Participant are required to perform a location verification utilizing the Voice Patrol® system by answering the call from or, calling the toll free number to the monitoring center supplied by Sentinel for the verification process. When a verification call is placed and answered, the system will play a brief welcome message and then instruct the answering party to "press any key to continue". The system will then prompt the enrollee to repeat two (2) paired number sequences called digit sets. Following the final response, the system will inform the enrollee that the verification session is completed. Verification sessions take approximately 15 seconds to complete.

IMPORTANT SENTINEL ADVANTAGE: Each verification session includes a ‘Liveness’ test. The Voice Patrol® system features the ability to randomly select one (1) of three possible digit sets therefore making it impossible for the participant to predict the required digit set and pre-record a verification.

IMPORTANT SENTINEL ADVANTAGE: The Voice Patrol® system analyzes each voice verification call against the participant’s voice template and automatically assigns a verification score from -100 (pure failure) to 100 (pure match). The Voice Patrol® system adds all successful verification calls containing high degrees of accuracy to the voice template therefore allowing the quality of a voice template to improve with every successful verification call from a participant.</td></tr>
<tr><td>10.14</td><td>Random Tracking</td><td>The verification process should also confirm the participant's location via the use of Caller ID/Automatic telephone Number Identification whereby, the computer will compare each telephone number the participant calls from against a listing of approved telephone numbers provided by the Officer at enrollment.</td><td>On all incoming calls, the Automated Number Identification (ANI) of the originating phone number is automatically validated against a list of approved authorized locations in addition to the verification of the individuals’ identity.

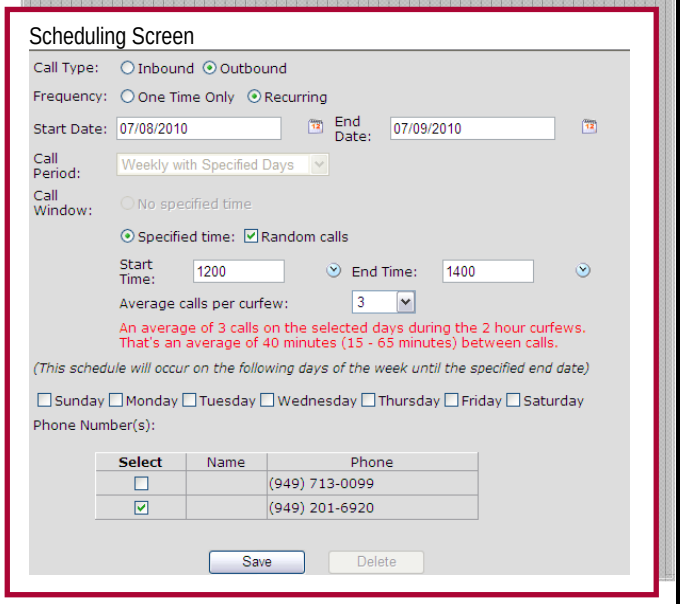
IMPORTANT SENTINEL ADVANTAGE: The Voice Patrol® system will not discontinue the verification call should the participant call from an unauthorized location but instead proceed with verifying the participant’s identity without informing the participant and provide the agency one of the following alerts providing positive confirmation of the methods in which the participant attempted to circumvent the system.
<table>
<tr><th>Description of Event</th><th>Event Trigger</th></tr>
<tr><td>Voice Verification Unauthorized Phone Number Verification Call Successful</td><td>Successful verification from UNAUTHORIZED phone number.</td></tr>
<tr><td>Voice Verification Unauthorized Phone Number Verification Call Failed</td><td>Unsuccessful verification from UNAUTHORIZED phone number.</td></tr>
</table></td></tr>
</table>

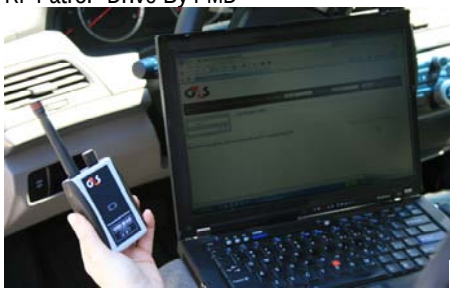
			IMPORTANT SENTINEL ADVANTAGE: The system will automatically log the unauthorized phone number to allow for the officer investigation to determine the actual physical location of the participant (should verification be successful) at that specific point in time.
10.15	Random Tracking	For participants where Caller ID/Automatic telephone number identifications does not operate, the tracking system should automatically request the telephone number from the participant, hang up, and then call the participant back at that number for verification. Vendors are to describe in detail how their system accomplishes this function.	**Sentinel meets this requirement.** If **Voice Patrol®** does not capture Caller ID/Automatic telephone number identifications, monitoring center staff can be prompted to request the telephone number from the participant, hang up, and then call the participant back at that number for verification.
10.16	Random Tracking	The system should be able to identify and differentiate between compliant responses, missed responses, late responses, system tampering/fraud, and unauthorized locations. The system must provide all unauthorized telephone numbers for Officer investigation.	**Sentinel exceeds this requirement.** **Voice Patrol®** system can to identify and differentiate between compliant responses, missed responses, late responses, system tampering/fraud, and unauthorized locations. **Voice Patrol®** records and stores all participant voice responses (compliant and non-compliant) and also allows authorized users to listen to voice messages left by participants through Sentinel's **SenTrak**, an advanced web-based information exchange platform. There are six (6) distinct types of failures identified by the **Voice Patrol®** system including a failed voice verification, calling from an unauthorized phone number, missing a scheduled/on-demand outbound call, missing a scheduled/on-demand inbound call, if a participant hangs up after answering or if the line is busy during the scheduled curfew time. Should any call result in any failure, the system will automatically generate a follow-up verification attempt or retry to the enrollee. **IMPORTANT SENTINEL ADVANTAGE:** The Voice Patrol® system will not discontinue the verification call should the participant call from an unauthorized location but instead proceed with verifying the participant's identity without informing the participant and providing positive confirmation of the methods (unauthorized location or having someone else call) in which the participant attempted to circumvent the system. Additionally, the system will automatically log the unauthorized phone number to allow for the officer investigation to determine the actual physical location of the participant (should verification be successful) at that specific point in time.

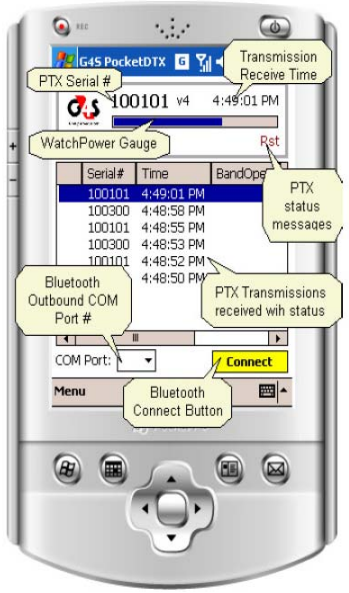
Through SenTrak, Sentinel provides alert notifications to its customers for a wide array of violations and events. When consecutive verification attempts fail, the system will create an exception and immediately generate a notification. The **Voice Patrol®** system supports four (4) different methods of alerting proper personnel of violations or exceptions including an immediate email message, a pager message or a telephone call to a specified supervisor. In addition to the immediate notification of an exception, the **Voice Patrol®** system can be configured to automatically generate an exception report every night at midnight. Any supervising agency can choose from the available four (4) notification methods or any combination of the four (4) to create agency specific notification profiles. The agency may choose to incorporate only one (1) notification profile or as many notifications profiles as deemed necessary for diverse monitoring needs. Should an agency choose to utilize multiple notification profiles then individual participant supervisors have the ability to select from the predetermined notification profiles on a per participant basis through SenTrak. For example, an officer can choose to receive only an email notification of violations for a particular participant but may choose to receive an email, a telephone call and a daily exceptions report of the violation for a different participant. Sentinel has provided a list of voice verification events available for notification in the following table:

Description of Event	Event Trigger
Voice Verification Call Successful	Successful verification from authorized phone number.
Voice Verification Call Failed	Unsuccessful verification from authorized phone number.
Voice Verification Unauthorized Phone Number Verification Call Successful	Successful verification from UNAUTHORIZED phone number.
Voice Verification Unauthorized Phone Number Verification Call Failed	Unsuccessful verification from unauthorized phone number.
Voice Verification Unscheduled Call Successful	Unscheduled successful verification received.
Voice Verification Unscheduled Call Failed	Unscheduled unsuccessful verification received.

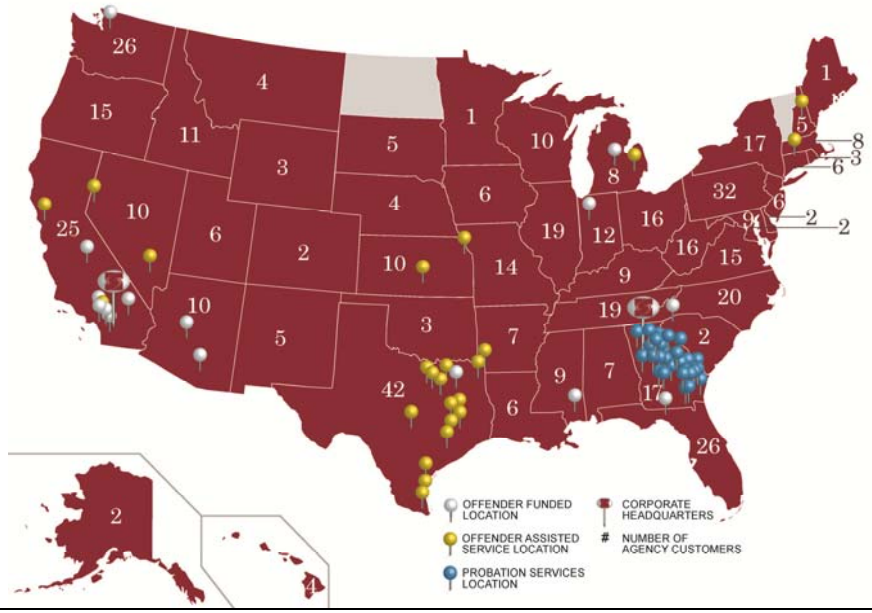
			Missed Voice Verification Call: Call window closed and no verification call was received or completed. (Default 20 minute delay before posting, in order to capture all calls and provide a window for those that are in progress.) Voice Verification Line Hang Up: Call was disconnected after Participant ID was entered. Voice Verification Outbound Call Line Busy: All outbound attempts reached busy line. Voice Verification Outbound Call No Answer: All outbound attempts reached no answer. (Voicemail and machines answering the line may produce different results.) Voice Verification On Demand Call Initiated: Sentinel staff initiates immediate outbound call. Voice Verification On Demand Call Inbound Call Initiated: Sentinel staff initiates immediate inbound call.
10.17	Random Tracking	Describe ability to initiate contacts at both random and scheduled intervals (up to 5 contacts per day).	**Sentinel meets this requirement.** Based on the call schedules entered during the pre-enrollment process, the **Voice Patrol®** system generates random and scheduled verification calls to the enrollee's monitoring locations up to five (5) times per participant per day. Sentinel's software system allows users to set curfew schedules on a per-participant basis, essentially establishing varying security levels. In other words, a user can assign riskier participants with more stringent **curfew schedules or less risky participants more lenient curfew schedules. The SenTrak system** allows for various combinations of verification schedules and validates all schedule combinations for the most robust curfew enforcement including: ✓ Inbound recurring each week on specific days due a specific time frame ✓ Inbound recurring daily, weekly, monthly or bi-monthly ✓ Inbound one-time at a specified time ✓ Outbound one-time at a specified time ✓ Outbound recurring at a specified time ✓ Outbound recurring at random during specified time frames

			The SenTrak software supports an unlimited number of schedules per participant, per day. A user is able to create schedules for participants through the simplified process illustrated by the monitoring screen to the right.  Users can suspend verification schedules for specified time periods and also specify the inbound or outbound telephone number that should be assigned to the schedule. All assigned schedules will be displayed in the system as active, pending activation, suspended, pending suspension or inactive. No schedule will ever be deleted from the system for audit and court testimony purposes and can also easily be reinstated at any time during monitoring.
10.18	Random Tracking	Describe ability for agency initiated calls (up to 5 contacts per day).	**Sentinel meets this requirement.** Based on the call schedules entered during the pre-enrollment process, the **Voice Patrol®** system can generate random, scheduled or on-demand outboard verification calls to the enrollee's monitoring locations up to five (5) times per participant per day. The SenTrak system allows for various combinations of outbound (agency-initiated) verification schedules including: ✓ Outbound one-time at a specified time ✓ Outbound recurring at a specified time ✓ Outbound recurring at random during specified time frames

10.19	Random Tracking	Describe ability for offender to initiate contact at both random and scheduled intervals (up to 5 contacts per day.)	**Sentinel meets this requirement.** Based on the call schedules entered during the pre-enrollment process, the **Voice Patrol®** system can accept inbound verification calls from the enrollee's monitoring locations up to five (5) times per participant per day. The SenTrak system allows for various combinations of outbound (agency-initiated) verification schedules including: ✓ Inbound recurring each week on specific days due a specific time frame ✓ Inbound recurring daily, weekly, monthly or bi-monthly ✓ Inbound one-time at a specified time
11.0	**CATEGORY 1 – RADIO FREQUENCY (RF) MOBILE (DRIVE BY) RECEIVER SPECIFICATIONS**		
Item	**Function**	**Description**	**Describe how Vendor passes, meets or exceeds**
11.1	Mobile Receiver	Deleted.	
11.2	Mobile Receiver	Deleted.	
11.3	Mobile Receiver	The Mobile Receiver should contain a multi-directional antenna with connector or an internal antenna, as well as a multi-directional antenna with a magnetic roof mount.	**Sentinel meets this requirement.** Sentinel's **Patrol Suite®** technology platform also includes the **RF Patrol® Drive-By** that incorporates a Portable Monitoring Device (PMD) and the Pocket PC. The Portable Monitoring Device (PMD) is a portable, hand-held, battery operated receiver unit with a multi-directional rubber-duck antenna with connector. The device detects and identifies all **RF Patrol®** transmitter (PTX2) signals in 300 to 500+ feet open field range. An officer can utilize this device on foot or in a surveillance vehicle. The PMD transmits data to the Pocket PC, a small hand-held device similar to a Personal Digital Assistant (PDA), via a Bluetooth connection for easy viewing. RF Patrol® Drive-By PMD 
11.4	Mobile Receiver	The Mobile Receiver should operate from an internal rechargeable battery for a minimum of 10 hours on a single charge and also be powered from both a vehicles cigarette lighter and 110 VAC	**Sentinel meets this requirement.** The **RF Patrol® Drive-By** PMD comes with 110VAC and 12VDC charging cables and is capable of multiple power functions including a stand-alone rechargeable battery that exceeds 10-hour capacity, a DC car cigarette lighter and an AC adaptor.

11.5	Mobile Receiver	The Mobile Receiver should receive transmitter events indicating the date, time, Participant's presence, tamper status and low battery.	**Sentinel meets this requirement.** The **RF Patrol® Drive-By** PMD detects and identifies all **RF Patrol®** transmitter (PTX2) signals in 300 to 500+ feet open field range and determines the condition of the transmitter with indicating the date and time stamps including tamper and battery status of the PTX2.
11.6	Mobile Receiver	The Mobile Receiver should provide prompts to the officer on transmitter ID number & tamper status. Vendor's proposal is to include a detailed listing of each prompt, its related cause, and describe how each is delivered to the Officer.	**Sentinel meets this requirement.** The PMD transmits data to the Pocket PC, a small hand-held device similar to a Personal Digital Assistant (PDA), via a Bluetooth connection for easy viewing. The Pocket PC is rechargeable through a standard wall or car charger and offers a LCD backlit display, a handheld case and quick signal recognition. This device's standard PDA design will allow officers to covertly verify a participant's whereabouts while walking or driving. The main display panel shows information about the last transmitter transmission received, including the transmitter serial number, its message version number, the date and time that the transmission was received, a gauge indicating the transmitter power and the **RF Patrol®** PTX status messages (Band Open, Tamper, Low battery, and Restart). RF Patrol® Drive-By Pocket PC 
11.7	Mobile Receiver	The Mobile Receiver should be equipped with a 500 event non-volatile memory that will time and date stamp the last 500 transmission signals. The information should also be downloadable to other computers. Describe your download capabilities.	**Sentinel meets this requirement. RF Patrol® Drive-By** Pocket PC list view displays the latest 100 transmitter transmissions received is available. The PMD can also be connected via PC computer to other computers.
11.8	Mobile Receiver	The Mobile Receiver should have a charge indicator.	**Sentinel meets this requirement.** Both the **RF Patrol® Drive-By** PMD and Pocket PC are equipped with a low battery indicator.
11.9	Mobile Receiver	The Mobile Receiver should have a battery level charge indicator.	**Sentinel meets this requirement.** Both the **RF Patrol® Drive-By** Pocket PC is equipped with a low battery indicator.

11.10	Mobile Receiver	The Mobile Receiver should have a power on/off switch.	**Sentinel meets this requirement.** Both the **RF Patrol® Drive-By** PMD and Pocket PC are equipped with a power on/off switch.

12.0	**CATEGORY 1 – RADIO FREQUENCY (RF) ELECTRONIC MONITORING SERVICE – OPTIONAL VENDOR PROVIDED OFFENDER SERVICES**	
Item	**Description**	**Describe how Vendor passes, meets or exceeds**
12.1	Vendor may offer and provide the following optional services/program for juvenile and adult Participants. Vendor should be experienced in and capable of delivering these services on a local, state, regional, and/or nationwide basis. Vendor shall be capable of providing staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Services and charges for those monitoring services may be negotiated based on each Agency's needs and may include any/all of the following services. Describe your company's experience, capabilities and resources to deploy each of these services.	**Sentinel exceeds this requirement.** In 20 years of service, Sentinel has provided a wide array of supervision services to offender supervision programs across the country including installation/retrieval services and full case management. **Sentinel monitors offenders that are pre-trial, post-sentence, and in custody at the local, state, regional, and nationwide level for those agencies it services, including both adult and juvenile populations.** **Sentinel provides uninterrupted 24 hour a day, seven (7) day a week, 365 days a year electronic monitoring and supervision services to more than 600 agencies across the United States. Sentinel's professional staff of 469 employees is solely dedicated to providing services within the offender management market providing monitoring to approximately 65,000 individual participants on a daily basis through its monitoring center.** Additionally, Sentinel is uniquely positioned to provide superior local services to its program due to its strong local presence in and around the United States. Sentinel also has extensive local presence through **its network of more than 50 field offices around the nation**. 

Sentinel's current service spectrum provides service options to distinct offender populations. Sentinel currently provides electronic home monitoring and probation services programs that entail compliance to court orders, and regular reporting to the department and/or the court through both an agency-funded model and an offender-funded model. (Please see response to specification 12.2 for Sentinel's extensive experience in offender-funded program models.) Sentinel provides installation and retrieval, limited- and/or full-case management programs where Sentinel on-site staff ensures that each participant must meet all terms of his and/or her sentence, including electronic supervision, payment of fees, fines, and restitution, and counseling or treatment, when needed. Sentinel continues to exhibit extraordinary depth in qualifications and experience. Sentinel will draw on its experience to provide a world-class program to successfully achieve the agencies goals and objectives of ensuring public safety and participant rehabilitation while giving access to new state-of-the-art technology.

Case supervision services are an integral component of the judicial process; therefore selecting the correct service provider is a critical decision. **Sentinel currently provides case management services to more than 100 programs from more than 50 locally-based offices across the country.** In these programs, Sentinel's staff monitors compliance to the court-ordered conditions

		with court orders via regularly scheduled meetings with each participant, addresses all issues of non-compliance, and reports continued non-compliance to the supervising agencies for resolution. Sentinel maintains individual case files on all participants for review by the court or its designees and in order to provide documentation for use in enforcement or revocation matters. Additionally, Sentinel has extensive experience customizing programs at the local level and currently **works directly with over 95 judges**. Through these programs, Sentinel's supervision services staff conducts more than **55,000 face-to-face defendant contacts a month**. Additionally, Sentinel understands the importance of expert court testimony and on a daily basis Sentinel has as many as **50 employees a day working in court rooms** nationwide testifying regarding participant activity. **This level of experience is difficult to replicate by any vendor and Sentinel is confident that its proposed program can exceed the court's expectations.**
12.2	Vendor should provide an Offender Funded Program for its Radio Frequency (RF) electronic monitoring equipment and services (including any optional Vendor provided offender services). The Vendor should assess the specified fee(s) to the offender and shall collect such fee(s) directly from the offender. Vendor should describe its program of fee assessment and collection and identify its charges for this program on the price sheet.	**Sentinel exceeds this requirement.** Sentinel has always been an innovator in its industry and **in fact pioneered the offender-funded program model** in response to changing industry needs. This model allows Sentinel to provide all of its monitoring services at little or no cost to the agencies, **thereby saving correctional agencies tens-of-millions-of-dollars in jail cost and monitoring fee avoidance**. Offender-funded electronic monitoring is Sentinel's core business operation and with no impact on operational budgets to fund these monitoring programs, agencies were able to further expand the programs without requiring additional funds to pay for monitoring services. Currently, Sentinel provides collection of fees from defendants and daily reporting to the court, **specifically for more than 45,000 offender-paid participants.** **Sentinel has monitored more than 1 million offender-paid electronic monitoring participants**. **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has directly collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers. **Sentinel will be responsible for invoicing and the collection of fees from all participants.** Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease

		court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc. Sentinel will collect fees from participants on a flat fee <u>or</u> sliding scale basis based on the following Offender Funded Program on the following characteristics: ▪ Minimum average of 100 active participant per installation area ▪ Average participant term on monitoring of 30 days ▪ 75 square mile installation area ▪ One Sentinel Installer/Case Manager per installation area ▪ Participants maintain a two-week advance payment ▪ 75% of participants willing to report to local Sentinel office for: ✓ Initial activation/orientation ✓ Equipment return ✓ Offender-fee payments ▪ Equipment/Monitoring/Notification consistent with that proposed for WSCA ▪ Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment. Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variances with any WSCA end user agency for Offender Funded Program Services. As previously stated, Sentinel pioneered the concept of offender-funded services and is highly experienced in incorporating a sliding fee scale model including the provision of services to participants that are deemed indigent. Sentinel has provided a detailed description of its program of fee assessment and collection in response to specifications 12.7 and 12.8, and identified its charges for this program on the price sheet.

12.3	Agency will maintain its own computers, software, and internet service for exchanging information.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for the maintenance of agency-owned computers, software and Internet service with the ability to connect to the proposed web-based monitoring platform, SenTrak.
12.4	The Agency will maintain complete responsibility for program management services not specifically listed.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all program management services not specifically listed in this section of the RFP 002012, Electronic Monitoring of Offenders.
12.5	The Agency will be responsible for all referrals of all new offenders to the program.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all responsible for all referrals of all new offenders to their programs.
12.6	Prior to any referral the Agency will ensure that the offender has a home phone or identifies the need of a cellular service monitoring unit.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for ensuring that all offenders referred to the program have an operational home phone or identifies the need of a cellular service monitoring unit.
12.7	Offenders should have an ability to pay for enrollment and services provided by the Vendor.	**Sentinel exceeds this requirement.** Sentinel understands that the objectives of offender-funded programs are to provide accountability to the participants through provision of selected court-referred programs and **ensuring each adult, with a demonstrated ability to pay, is responsible for payment for electronic home monitoring**. An important segment of the Intake and Orientation Meeting are the financial assessment and fee payments. Using the approved fee schedules as set forth in the pricing section based on the financial assessment process detailed as the response to specification 12.8, Sentinel will review the costs of the program, ensure all required payments have been made and receive any payments scheduled at this time. Currently, Sentinel provides collection of fees from defendants and daily reporting to the court, **specifically for more than 45,000 offender-paid participants.** Sentinel pioneered the concept of offender-funded services and is highly experienced in incorporating a sliding fee scale model including the provision of services to participants that are deemed indigent. For those participants that show inability to pay full program fees after all the above elements have been considered, Sentinel will offer a discounted rate off of the full program fees to the participant. The rate will be based on an assessment of the participant's ability to pay. Should the participant not agree with the assessment and discounted rate, Sentinel will provide its finding to the participating agency/courts for recommendations on how to proceed. Sentinel understands that no offender can be denied access to the program based on their

inability to pay. **Sentinel will use the following strategies to ensure successful collections:**

- Sentinel local staff will address the importance of keeping current with all program fees and each participant will be required to sign an agreement which outlines program fees and how and when program fees are to be submitted.
- Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc.
- **IMPORTANT SENTINEL ADVANTAGE:** Sentinel will also offer an optional on-site Kiosk that will allow offenders to pay monitoring fees electronically. **PLEASE NOTE:** Through this kiosk, Sentinel can offer an optional service to allow offenders to pay other fees owed to the participating agency or other county/city/state agencies such as parking tickets, court fines or restitution.
- Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason.
- Sentinel local staff will promptly follow-up on missed or partial payments.
- Sentinel will reassess the financial conditions for those participants who have experienced a sudden change in income in order to reevaluate if the participant's ability or inability to pay the established and agreed upon program fees warrant a reduction in fees.

		▪ Sentinel will use collection agencies if needed in order to recoup established program fees. ▪ Sentinel will provide monthly reports to the participating agency and/or courts that provide details on fees collected from the offender funded program. ▪ Sentinel will also provide a report that will detail Sentinel's efforts for collecting fees from delinquent participants. ▪ Sentinel will immediately advise the participating agency and/or courts on any offender's refusal to pay program fees to see about having the participant removed from the program. **IMPORTANT SENTINEL ADVANTAGE:** All participant payments made to Sentinel are processed through Sentinel's proprietary SenTrack software and made available to the participating agencies or courts via this automated software interface and in hard copy reports/invoices. Within this system, Sentinel will track the progress of participant payments as well as alcohol test results, drug screens, report dates, and other court order conditions that may be required by or beyond the Scope of Work for this program. All activity is automatically time- and date-stamped within the software for chronological integrity purposes. SenTrack case management software allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software.
12.8	Vendor will make arrangements to create a fee payment assessment whereby the cost of the program to offenders will be set on a mutually agreed upon schedule based on monthly earnings of an offender.	**Sentinel exceeds this requirement.** Sentinel recognizes the budget concerns facing agencies nationwide. The challenges of providing thorough supervision within budget constraints have resulted in many localities charging the cost of electronic monitoring and re-entry programs back to participants in an effort to stretch budgeted electronic monitoring dollars. More importantly, Sentinel's experience with offender-paid programs indicates that some level of payment for service, regardless of the amount, is a strong enhancement in the performance of the participant in the program, resulting in a substantial reduction in recidivism. **Sentinel is experienced in offender-funded programs and has processes and systems in place that presently charge thousands of participants nationwide for the cost of their own electronic supervision** allowing agencies to save time and valuable resources by relieving the internal administrative burden of collecting, tracking and reporting offender fees.

Sentinel has always been an innovator in its industry and in fact **pioneered the offender-funded program model** in response to changing industry needs. This model allows Sentinel to provide all of its monitoring services at little or no cost to the agencies, **thereby saving correctional agencies tens-of-millions-of-dollars in jail cost and monitoring fee avoidance**. Offender-funded electronic monitoring is Sentinel's core business operation and with no impact on operational budgets to fund these monitoring programs, agencies were able to further expand the programs without requiring additional funds to pay for monitoring services. This is a program model that Sentinel has used with great success since 1992, and **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers.

When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services. Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors:

(1) Present financial position.

(2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position.

(3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program.

(4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision.

Sentinel is the most experienced in the industry in managing offender funded programs based on a sliding-scale fee structure for those participants identified as indigent. Sentinel has the ability to offer a graduated fee scale available to the WSCA participating agencies for determination of reduced fees to be collected for an indigent participating offender where some participants will be able to pay the full program fees while some will only be able to pay a portion of the daily fees or no fees at all.

Sentinel will collect fees from participants on a flat fee <u>or</u> sliding scale basis based on the following Offender Funded Program on the following characteristics:

		Sentinel will collect fees from participants on a flat fee or sliding scale basis based on the following Offender Funded Program on the following characteristics: ▪ Minimum average of 100 active participant per installation area ▪ Average participant term on monitoring of 30 days ▪ 75 square mile installation area ▪ One Sentinel Installer/Case Manager per installation area ▪ Participants maintain a two-week advance payment ▪ 75% of participants willing to report to local Sentinel office for: ✓ Initial activation/orientation ✓ Equipment return ✓ Offender-fee payments ▪ Equipment/Monitoring/Notification consistent with that proposed for WSCA ▪ Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment. Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variances with any WSCA end user agency for Offender Funded Program Services. **Sentinel has a current financial assessment procedure and participant forms already in use at other various agencies as well as proven invoicing and fee collections procedures in place to ensure program success right out of the gait should any agency choose to utilize these services.** The methodology used by Sentinel for determining offender-funded fees is based on Sentinel's extensive experience, performance and success in providing these services to other criminal justice entities. Sentinel will conduct a financial assessment for every offender who has been determined eligible for the program by the participating agencies/courts. Sentinel's financial assessment process takes into consideration the participant's current and future financial status when determining a participant's ability or inability to pay the daily maximum as established in the sliding fee scale table that is based on the adjusted annual household income.

12.9	Offenders will be responsible for the cost of lost, damaged, or stolen equipment.	**Sentinel meets this requirement.** Sentinel understands that program participants will be responsible for the cost of lost, damaged, or stolen equipment. Sentinel will directly bill all participants for equipment that was lost, stolen damaged. Based upon Sentinel' experience in other contracts, Sentinel has found a few points essential to improved management of equipment inventory and loss, damaged or stolen equipment. This includes increased emphasis to not remove the transmitter until all pieces of equipment provided to the participant are together in the same place, either at the participant's home or the Sentinel office. Sentinel would request ongoing coordination with the participating agencies for participants to return equipment to Sentinel Office.
12.10	**The Vendor should provide limited case management services to include:**	**Sentinel exceeds this requirement. Sentinel is proposing several value-added options to help elevate the burden of routine program management, installation/retrieval service, compliance monitoring, inventory management and fee collections from WSCA participating agency employees allowing officers more time to manage violations and provide needed case management to its offender population.** Sentinel provides options for both **limited or full-service case management** in addition to installation and retrieval services will allow both agencies to simply refer participants to Sentinel and receive violation notifications for all program participants through immediate automated or manual notifications. Sentinel is committed to providing a continuum of case management operations to WSCA participating agencies that would allow for Sentinel staff to be located on-site for program operation. In addition to the standard requirements of this RFP, Sentinel is also proposing a completely offender funded program that would allow participating agencies to avoid collecting fees directly from program participants. Sentinel's case management model would allow for a full time office to be opened and local staff to be hired and trained. Once established this location could be utilized by participating agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand your programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates. Sentinel has extensive experience provide the following staff members to programs utilizing its limited- or full-service case management services:

		Program Director: Dependent on the size of the specific program, Sentinel may employ a Program Director as the lead contact for the daily operation of the program and handle any court requests. The candidate will hold at minimum a Bachelor's Degree in social work or counseling and have counseling or social work experience with participants. This person's duties will include: ▪ Daily reconciliation of all payments received ▪ Supervision of all Sentinel office staff ▪ Quality assurance audits and reviews of supervision methodologies ▪ Oversee all contacts with victims ▪ Investigate all participants grievances ▪ Daily liaison for court personnel ▪ Court representative for any proceedings for participants ▪ Steering committee representative for Sentinel with court/agency personnel **Case Manager(s):** Case Manager candidates will also hold at minimum of a Bachelor's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include: ▪ Adhering to Sentinel's Case Management Model including performing (1) Assessment, (2) Interpretation, (3) Case Planning, (4) Ensuring the Delivery of Services and (5) Evaluating Performance ▪ Explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature ▪ Create and maintain files on all participants referred to the program ▪ Process all payments ▪ Communication with court personnel if there are any inquiries on a specific participants ▪ Perform notifications of program completions/non-compliance **Administrative Assistant:** Depending on the size of the specific programs and the volume of tasks placed on an office providing this type of service to a participant population, an Administrative Assistant maybe needed. This person will:

- Handle all calls received at the office
- Provide assistance to the Program Director and Case Manager(s) as needed
- Assist with performing any required transmission of reports
- General office tasks

IMPORTANT SENTINEL ADVANTAGE: Sentinel designed its proprietary, web accessible case management software, SenTrack, specifically for use in the offender services arena. Employing SenTrack allows **real-time, on-line web accessibility** to participant case information and reports for Sentinel employees **and** authorized participant agency and/or court personnel. As the SenTrack case management software is an in-house concept and design, SenTrack is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support and recommends all participating stakeholders have access to the SenTrack software for program review and oversight.**

Sentinel catapulted the speed, capacity and capabilities of case management software through the development of the SenTrack SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective. **This translates into the ability to modify or develop new software variations as may be needed for the agency directly, in house, without having to utilize outside vendors which may bring data security concerns to the agency. Only Sentinel personnel would have access to the confidential participant data and the development of any new application.**

Sentinel's SenTrack case management software incorporates all of the technology offered by Sentinel including the Kiosk. The software is fully integrated in every Sentinel branch office and has become the foundation from which Sentinel serves its customers. Highlights of the SenTrack case management software include:

- Internet accessibility; available 24 hours a day to any Sentinel customer
- All client obligations to the court are tracked (courses, fines, drug screens, community service, restitution, demographics etc.)
- Real-time communication with Kiosks
- On-line payment acceptance
- Proprietary Case Management Software; 100% in-house support and customization available

- Over 150 available reports
- Customized reports provided at **no cost**
- Currently services more than 200 agencies and over 45,000 offender-paid participants
- Able to capture photo images as required
- Fully redundant and supported by continuous operation monitoring center designed to Underwriters Laboratory specifications
- Internal audit tools track all changes
- Unlimited query capabilities for detailed statistical reporting

The SenTrack system is completely customizable and currently provides more than 150 different types of case management and financial reports. Through the ability to customize the system, SenTrack has made it possible for judges to have the reports they want in the format they desire.

IMPORTANT SENTINEL ADVANTAGE: Sentinel has helped pioneer the concept of opening local, community-based "Success Centers" where probationers/defendants/parolees can participate in electronic monitoring programs and optionally receive assistance with job placement, address drug addiction, as well as participate in cognitive skills classes, anger management and other developmental programs. Using this model, Sentinel can work directly with the participating agency and the courts to develop additional programs at its Success Center to help reduce recidivism **AT NO COST TO THE AGENCY**. Sentinel's basic business model rests on proven research that has shown that heavier punishment and long terms of incarceration or probation are not lasting answers to stem criminal behavior. Rehabilitation-oriented programs and defendant accountability, combined with community-based intervention and support, is the more sensible way to tackle this complex issue.

Should participating agencies elect to utilize the Success Center Model, Sentinel will additionally provide the following staff members:

Program Specialist(s): Program Specialist candidates will hold at minimum a Master's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include:

- Delivery of daily classes based on Diversion Orders or needs assessments
- Communication with the Project Director/Case Manager(s) regarding each defendants progress regarding his or her Case Plan
- Maintaining current on all applicable laws and changing regulations for class delivery

12.11	a. Work/school verification	**Sentinel exceeds this requirement.** Sentinel will verify all pre-approved locations including work, school, college, counseling, AA/NA, victim awareness or other program classes and capture teacher/supervisor information for additional follow-up.
12.12	b. Schedule entry/management	**Sentinel meets this requirement.** Sentinel Project Director/Case Managers will profile new participant enrollments, perform all schedule entry and schedule management. The electronic monitoring program will continuously monitor participants within their assigned schedules as determined by the participating agencies/courts. When enrolling participants, Sentinel Case Managers will set up curfew information on a per participant basis in the SenTrak software. The SenTrak software supports an unlimited number of curfew/absence periods per client, per day and will allow authorized users to create, edit and delete all parameters for individual participants.
12.13	c. Collateral office visits to review compliance, adjust schedules, collect fee(s).	**Sentinel exceeds this requirement.** Sentinel understands the importance of having a robust, accountable process to ensure that participants referred into the program are held accountable and are treated fairly and with respect while participating in the program. During regularly scheduled office visits, Project Director(s)/Case Manager(s) will periodically review the participant's file for the duration of the participant's time in the program to review participant compliance, adjust schedules and collect fee(s). The proposed program includes regular check-in and contacts that will allow the participant the ability to show accountability and proactively advance through the program. It has been proven that regular check-ins in the early program stages and throughout the program have led to more successful outcomes. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel services include the incorporation of the latest technological advancements in the defendant services arena including Sentinel's Kiosk check-in and reporting capabilities, Sentinel's latest electronic monitoring equipment and formalized collections programs. All of these tools and technologies can be incorporated in the provision of WSCA participating agency programs including multi-level supervision and fees determined by the defendant's case requirements

		IMPORTANT SENTINEL ADVANTAGE: Sentinel services include the incorporation of the latest technological advancements in the defendant services arena including Sentinel's Kiosk check-in and reporting capabilities, Sentinel's latest electronic monitoring equipment and formalized collections programs. All of these tools and technologies can be incorporated in the provision of WSCA participating agency programs including multi-level supervision and fees determined by the defendant's case requirements **Kiosk Participant Check-in and Collection Locations:** The Centurion Kiosk was developed by Sentinel to provide an interactive and automated solution for participant check-ins that confirms identity through fingerprint identification and permanently records date and time of check-in. For limited or full-service case management programs, kiosks can be placed at the Sentinel offices, agency locations or at remote locations for participants to check-in as needed. The advanced functionality of the Kiosk enables participants to check-in, update demographic information and compliance status, receive messages from program administrators, and submit payments for fines / fees / restitution. The results submitted by participants through the Kiosk can be pushed to the participating agency's system. Kiosk
12.14	d. Participant initial contact	**Sentinel meets this requirement.** As part of Sentinel's provision of full service programs, Sentinel utilizes the services of the Sentinel Enrollment Department. This team handle can handle all new enrollment duties with program participants. For this project, they can be the first tier of contact with a defendant **(if not referred to Sentinel's office directly after court)** that would allow us to inform the defendant of all program requirements prior to enrollment in the event that they had any questions. Sentinel's Enrollment Department can assist with new enrollments for these programs when appropriate to ensure efficient local office operations. **Intake Process:** When a participant is referred to the house arrest electronic monitoring program, he or she is expected to report to the program within one (1) business day to begin services but no later than 72 hours from referral. The first time the participant reports to Sentinel's office, the Project Director/Case

		Manager completes the standard Intake Form and enters the participant's information in SenTrack, Sentinel's unique electronic case management system. During this interview, the Project Director/Case Manager will collect information using Motivational Interviewing techniques which are extremely important during the participant's first encounter with the Project Director/Case Manager. From the moment the participant enters the office, the participant will be made aware that he and/or she is welcomed in the program and that the program exists to help the participant succeed in completing his or her sentence.
12.15	e. Participant orientation	**Sentinel meets this requirement.** Sentinel's Project Director/Case Manager(s) will be responsible for conducting an Intake and Orientation meeting with each program participant to complete all set-up and system requirements with the person sentenced or placed on the home detention electronic monitoring program at the participant's home, place of business or other location(s) as determined by the participating agency/court. The orientation is the most important appointment held with the participant as it sets the parameters of the participant's monitoring and program regulations. Sentinel's Project Director/Case Manager(s) will collect and verify all of the necessary participant documentation and information to verify the participant's employment, community restitution, treatment classes, religious activities, funeral services, medical appointments and any other activities the person participates in on an on-going basis. In addition to confirming the participant's information, all permitted activities and required verification/ documentation including reasons for possible termination from the program would be explained to the participant so that there were no misunderstandings. **Please note:** Sentinel understands it may not terminate any person's participation with the program without first notifying the participating agency/court and receiving correspondence from the participating agency/court giving Sentinel permission to terminate the person from the home detention electronic monitoring program. During this meeting Sentinel will: ▪ Obtain a copy of the Pre-conviction or conviction from the participant, jail and/or court

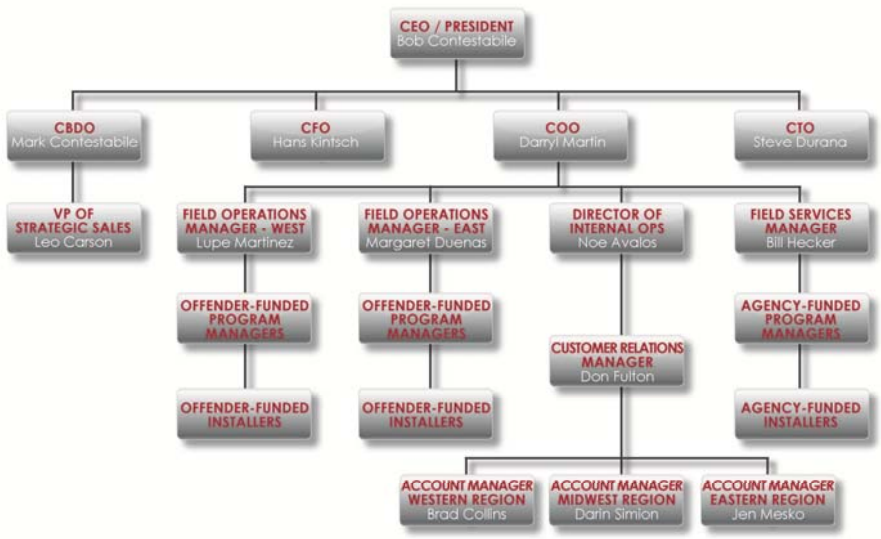
		▪ Verify participant's name, date of birth, home address, telephone number, race and family details ▪ Verify court details including docket number, assigned judge, date of the court order, anticipated date of execution of sentence and restitution requirements ▪ Capture participant photograph and signature ▪ Obtain signature of participant consent for the Authorization for Information Release (if required) ▪ Complete a financial assessment of the participant to determine indigent status (if required) ▪ Complete a risk/need assessment to determine the participant's Case Plan (if full-service option selected) ▪ Inform the participant of the days they are required to report into the office for face-to-face meetings ▪ Review required restitution and fee payments Another important segment of the Intake and Orientation is the fee payments. Using the approved fee schedules as set forth herein, Sentinel will review the costs of the program as well as any restitution payment requirements, ensure all required payments have been made and receive any payments scheduled at this time. Sentinel Project Director/Case Manager(s) will explain the fee structure and inform the defendant that his or her case will be completion only if he or she complies with the conditions, completes all program requirements and has already paid all restitution owed to the victim and all fees. For either limited or full-service case management models, Sentinel **recommends** that at a minimum the goals for the house arrest electronic monitoring program should include successful completion of court mandated rehabilitation programs including (e.g. domestic violence programs, education classes, GED preparation, life skills training, mental health counseling/treatment, parenting classes, substance abuse counseling/treatment and other classes deemed necessary), timely arrival at all meetings/programs and maintenance of timely payments. **After providing thorough explanations of both the program parameters and the fee structures, Sentinel Project Director/Case Manager(s) will obtain a written agreement from each participant prior to enrollment, indicating the participant agrees with all conditions of the home detention electronic monitoring program.**

12.16	f. Activate and install devices on offenders/participants.	**Sentinel meets this requirement.** During the Intake and/or Orientation meeting, the Project Director/Case Manager(s) will install and activate all necessary electronic monitoring equipment on the participant. Sentinel can offer a full continuum of electronic home monitoring equipment to monitor and verify that program participants remain at home/work during specified time periods and shall report unauthorized absences, late returns, equipment malfunctions, verbal responses and other functions to a central computer system.
12.17	g. Monitoring of Participant with notification to Officer of violation by automated and non-automated methods.	**Sentinel meets this requirement.** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately or upon expired grace period. Sentinel supports all standard methods of notification, such page (alpha or numeric), electronic mail, fax, and/or text message to a cell phone. **Manual Voice (Manual Screening/Triage):** In addition to automated notifications, Sentinel can continue to offer triage via monitoring center staff where live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . At no additional cost, Sentinel will customize each individual participating agency's notification profiles to include grace periods for specified violations before the system generates notification should the agency request this service.
12.18	h. Field Service Calls/ Maintenance of equipment	Sentinel exceeds this requirement. **Field Service:** Sentinel has a proven track record of providing excellent performance and flexibility to its customers and will continue to commit this same dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all field services including but not limited to on-site technical assistance and 24 hour a day customer support as well as inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members

that add significant value.

IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of **Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness.

Sentinel's extensive depth of field services personnel (as shown on the following organizational chart) will provide corporate oversight for the contractual cycle of each of the participating programs during the program lifecycle. The assigned field services personnel will be dispatched to provide on-site service in the event of the need for electronic diagnosis or replacement of component problems. Field services personnel will also be responsible for scheduling training, per the contract, with agency staff on the use of equipment and reading reports. This strong nation-wide presence of qualified Sentinel staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract.



Additionally, staffed monitoring services and technical support are available from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.**

Maintenance: Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems including **RF Patrol®** and confirms that all equipment provided to WSCA participating agencies will be covered by a full manufacturer's warranty **for the length of any contract**. Sentinel will maintain all equipment in good operating condition and free from materials defects and/or workmanship under normal and proper use for the term of this agreement.

Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. Sentinel's assigned Account Manager will work proactively with each Western States Contracting Alliance participating agency to ensure the appropriate amount of equipment and spares are maintained for the electronic monitoring of offenders. This open communication allows Sentinel to provide equipment in a timely manner without having to depend on costly overnight / express delivery in order to meet the program's equipment needs.

Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program

		expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. Additionally, if any agency's spare inventory is depleted, Sentinel will re-supply the appropriate equipment via overnight delivery at no additional cost within 24 hours after notification. All shipping costs (both delivery and return) of all equipment and supplies will be the responsibility of Sentinel. **Product Warranty:** Sentinel represents and warrants that, upon delivery of any product and/or consumable to the delivery location, such product will have been manufactured, filled, packaged, stored and shipped materially in accordance with the specifications or custom specifications for such product in accordance with the associated purchase order. Sentinel further represents and warrants that it shall obtain and maintain all necessary licenses, permits or approvals in connection with the manufacture, filling, packing, testing, storage and shipment of each such product. **Sentinel warrants all of its equipment and software for the life of the contract.** This includes software maintenance, licensing and future feature enhancements. **Warranty Service:** Warranty service with Sentinel is a very simple process. The participating agency only needs to contact the proposed Account Manager to discuss warranty service and/or feature upgrades. Sentinel is committed to the continual development of feature enhancement and product development. The Account Manager will also work with the Sentinel training department to provide any training required by a new feature or upgrade to the equipment or system.
12.19	i. Optional mobile spot check of Participant	**Sentinel meets this requirement.** Sentinel can provide random spot checks of participants while away from the home utilizing the **RF Patrol® Drive-by as described more thoroughly in Specifications 11.3 – 11.10**.

	OPTIONAL SERVICES	**Optional Sentinel Kiosk for Random/Scheduled Tracking** Sentinel proposes an on-site kiosk as an optional form of Random/Scheduled Tracking and/or Offender Fee Collections. The Kiosk will allow offenders to report, check-in and/or pay monitoring fees electronically. **PLEASE NOTE:** Through this kiosk, Sentinel can offer an optional service to allow offenders to pay other fees owed to the participating agency or other county, city, state agencies such as parking tickets, court fines or restitution. The pptional Sentinel Kiosk for Random/Scheduled Tracking, Reporting & Offender Fee Collections is included on the Price Worksheets as an Optional / Additional Radio Frequency (RF) Electronic Monitoring Service.

SPECIFICATIONS

These specifications are the minimum. The vendor has listed, clearly demonstrated, and presented features that add value, savings and/or reliability.

CATEGORY 2 – ALCOHOL MONITORING EQUIPMENT AND SERVICE AND ALCOHOL MONITORING TRANSDERMAL EQUIPMENT AND SERVICE			
1.0	**SECTION A General Experience Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
1.1	General Experience	The proposed device must have been in use and installed on offenders through one or more contracts with County, State or Federal Government agencies. This experience must have been within the past six (6) consecutive months prior to the proposal submittal date. Anytime Beta testing does not count toward the required experience.	**Sentinel exceeds this requirement. Sentinel has over 20 years direct experience delivering alcohol monitoring solutions to criminal justice agencies. Furthermore, Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel is proposing solutions for both Alcohol Monitoring and Transdermal Alcohol Monitoring that include the latest generation, most advanced MEMS/MEMS3000 (also known as 3M Remote Alcohol Monitoring System) for Alcohol Monitoring and SCRAM/SCRAMx (from Alcohol Monitoring Systems, Inc.) for Transdermal Alcohol Monitoring. Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. These alcohol monitoring solutions and accompanying software have been in continuous use for more than six (6) years in agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both the MEMS and SCRAM alcohol monitoring solutions in the Appendix D: Bidder Information and Profile section of this proposal as required. Sentinel has additionally proposed multiple optional technologies and services in both categories, including but not limited to Sentinel's: VI-CAP Patrol™ Alcohol Monitoring, VI-CAP Patrol™ Mobile Cellular Alcohol Monitoring, and CAM Patrol Plus™ Transdermal Alcohol Monitoring.

			Sentinel has been providing electronic monitoring and participant supervision for more than 20 years since its founding in 1992, including the MEMS breath alcohol monitoring solutions for the past 20 years, and SCRAM transdermal alcohol for the past six (6) years. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel has over 20 years direct experience delivering MEMS alcohol solutions to criminal justice agencies. At twenty years, Sentinel's experience delivering MEMS services is nearly 10 times that of 3M, who first entered the electronic monitoring market less than approximately two years ago. Sentinel is still currently in the business of providing electronic monitoring services to community corrections and/or criminal justice organizations and since its inception has had more than 1,000,000 participants successfully completed their programs through Sentinel's extensive continuum of community-based monitoring services.
1.2	General Experience	The proposed device must have been installed and in use on at least an aggregate of 500 offenders through one or more contracts with County, State or Federal Governmental agencies. This experience must include at least six (6) months of active monitoring for the model offered in response to this RFP. The vendor's experience shall have been met with the vendor acting as the prime contractor in providing all of the above services. Identify these agencies, volumes and devices in your proposal response.	**Sentinel exceeds this requirement. Sentinel has over 20 years direct experience delivering alcohol monitoring solutions to criminal justice agencies. Furthermore, Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel is proposing solutions for both Alcohol Monitoring and Transdermal Alcohol Monitoring that include the latest generation, most advanced MEMS/MEMS3000 (also known as 3M Remote Alcohol Monitoring System) for Alcohol Monitoring and SCRAM/SCRAMx (from Alcohol Monitoring Systems, Inc.) for Transdermal Alcohol Monitoring. Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. **These alcohol monitoring solutions and accompanying software have been in continuous use for more than six (6) years in agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both the MEMS and SCRAM alcohol monitoring solutions in the Appendix D: Bidder Information and Profile section of this proposal as required.**
1.3	General Experience	The proposed software must have been in	**Sentinel exceeds this requirement. Sentinel has over 20 years direct**

		use at least six (6) consecutive months through one or more contracts with County, State and Federal Government agencies. Anytime Beta testing does not count toward the required experience.	**experience delivering alcohol monitoring solutions to criminal justice agencies. Furthermore, Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring contractor for more than 11 years since the WSCA contract's inception.** Sentinel is proposing solutions for both Alcohol Monitoring and Transdermal Alcohol Monitoring that include the latest generation, most advanced MEMS/MEMS3000 (also known as 3M Remote Alcohol Monitoring System) for Alcohol Monitoring and SCRAM/SCRAMx (from Alcohol Monitoring Systems, Inc.) for Transdermal Alcohol Monitoring. Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. **These alcohol monitoring solutions and accompanying software have been in continuous use for more than six (6) years in agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both the MEMS and SCRAM alcohol monitoring solutions in the Appendix D: Bidder Information and Profile section of this proposal as required.**
1.4	General Experience	The Vendor shall provide a secure confidential monitoring service center and help-desk facility. 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 Government agencies at the time of proposal submittal. This experience shall be with the same government agencies listed in Item 1.2. The Vendor shall have been the prime contractor for any contract services performed by any subcontracted monitoring service center or help-desk facility.	**Sentinel exceeds this requirement. IMPORTANT SENTINEL ADVANTAGE: Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring outsource monitoring services/help desk services to third-party providers for both radio frequency monitoring and alcohol monitoring thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.) **Sentinel has over 20 years direct experience delivering alcohol monitoring solutions to criminal justice agencies. Furthermore, Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring contractor for more than 11 years since the WSCA contract's inception.**

			Sentinel is proposing solutions for both Alcohol Monitoring and Transdermal Alcohol Monitoring that include the latest generation, most advanced MEMS/MEMS3000 (also known as 3M Remote Alcohol Monitoring System) for Alcohol Monitoring and SCRAM/SCRAMx (from Alcohol Monitoring Systems, Inc.) for Transdermal Alcohol Monitoring. Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. **These alcohol monitoring solutions and accompanying software have been in continuous use for more than six (6) years in agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both the MEMS and SCRAM alcohol monitoring solutions in the Appendix D: Bidder Information and Profile section of this proposal and referenced in Item 1.2 as required.** **The Sentinel secure confidential monitoring center and help desk have been servicing WSCA participating agencies as a prime contractor since 2002 (over 11 years). Sentinel understands the objectives of the Western States Contracting Alliance program better than any other vendor in the industry.** **The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis.** The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted, monitoring information is disseminated and technical support (help desk) services are provided to all Sentinel customers including those listed in Appendix D: Bidder Information and Profile section of this proposal and referenced in Item 1.2.

Sentinel Irvine Facility

Sentinel operates both its primary monitoring center located in California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. To maintain monitoring center operational integrity and confidentially, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards:

- Enforces an electronic key card system for entryway access to both outside building and monitoring center
- Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways
- Archives data daily and stores it in a secure location to protect against memory loss in case of power failure

Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.

			The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** The Western States Contracting Alliance participating agencies can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year. Sentinel strives to resolve any customer inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services,

			during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Account Manager/Field Operations Manager for customer enhancement requests, suggestions and ideas.
1.5	General Experience	The Manufacturer shall have an ISO 9001 certification.	**Sentinel exceeds this requirement.** Much of Sentinel's success hinges on Sentinel's top management's commitment to continual process improvements, which is a main goal of the ISO 9001:2008 Quality Standard. **Sentinel's manufacturing division received ISO 9001-2008 accreditation in January 2009, the manufacturer of the MEMS 3000 device received certification in 1997 and the manufacturer of the SCRAMx device received certification in 2012.** Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments and to ensure all staff has access to needed resources and training to support the quality management system. Sentinel has provided copies of the certifications in the Exhibits section of this proposal.
1.6	General Experience	All devices shall be currently registered and approved by the Federal Communications Commission (FCC).	**Sentinel meets this requirement.** All of the proposed equipment complies with all appropriate FCC regulations. Sentinel has provided the Identifier Numbers below and copies of the certifications are included in the Exhibits section of this proposal: **Part 15** ▪ MEMS3000 Home Station ▪ SCRAMx Bracelet P8M-SM02

			▪ SCRAMx Base Station P8M-SM03 **Part 68** ▪ MEMS3000 Home Station ▪ SCRAMx Base Station US:AMSMM00BSM0
2.0	**SECTION B Monitoring Center Facility and Monitoring Center Interactive Services**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
2.1	Services	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 Government agencies at the time of proposal submittal. This experience shall be with the same government agencies listed in Item 1.2. The Vendor shall have been the prime contractor for any contract services performed by any subcontracted monitoring service center or help-desk facility.	**Sentinel exceeds this requirement. IMPORTANT SENTINEL ADVANTAGES:** ▪ **Sentinel has over 20 years direct experience delivering alcohol monitoring solutions to criminal justice agencies. Furthermore, Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring contractor for more than 11 years since the WSCA contract's inception, including the Sentinel secure confidential monitoring center and help desk that have been servicing WSCA participating agencies as a prime contractor since January 2, 2002 (over 11 years). Sentinel understands the objectives of the Western States Contracting Alliance program better than any other vendor in the industry.** ▪ **Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring outsource monitoring services/help desk services to third-party providers for both radio frequency monitoring and alcohol monitoring thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.) **The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis.** The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000

			square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted, monitoring information is disseminated and technical support (help desk) services are provided to all Sentinel customers including those listed in Appendix D: Bidder Information and Profile section of this proposal and referenced in Item 1.2. **Staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** The Western States Contracting Alliance participating agencies can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year. Sentinel strives to resolve any customer inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for

			resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Regional Account Manager/Field Operations Manager for customer enhancement requests, suggestions and ideas.
2.2	Facility	The Vendor's Monitoring Center should have a permanently installed and functioning emergency backup power source, independent of its main power source, capable of maintaining continuous operations, for a minimum of forty-eight (48) hours, in the event of failures of normal utility power. If power is not restored, a back-up monitoring center service is activated within 60 minutes.	**Sentinel exceeds this requirement. Sentinel's monitoring centers have permanently installed and functioning emergency backup power sources, independent of its main power source, capable of maintaining continuous operation until primary power is restored or the backup monitoring center is fully functional.** Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-the-art technology including: ▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator. Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's on-site diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. Once operating, Sentinel's generator can provide

			power for the entire monitoring center for up to 10 days or longer if refueled. The diesel generator is regularly inspected to ensure that it remains in operational order at all times. **Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days (in excess of 72 hours). Sentinel has never lost any data or performance capability due to power losses of any sort.**
2.3	Facility	The Vendor's Monitoring Center should have ventilation and temperature controls adequate to ensure proper functions of the monitoring center hardware.	**Sentinel meets this requirement.** The continuously staffed Sentinel monitoring center resides in independently secured, climate-controlled, properly ventilated facilities with raised floors to ensure proper functions of the monitoring center hardware and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community.
2.4	Facility	The Vendor's Monitoring Center's physical security features at a minimum should include closed circuit camera system and limited access doorways. Describe other features to ensure physical security.	**Sentinel exceeds this requirement.** To maintain monitoring center operational integrity, and physical security, Sentinel's monitoring center's physical security features include closed circuit camera system and limited access doorways. Each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the

			general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified.
2.5	Facility	The Vendor shall have a secondary (backup) Monitoring Center 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	**Sentinel exceeds this requirement.** Sentinel has a redundant monitoring center located sufficiently distant from the primary center, that 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. To support business operations for electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a fully-redundant monitoring center. Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart so it will be unaffected by a manmade or natural event or loss of electrical or communications services that would disable the primary

		would disable the primary Monitoring Center.	monitoring center. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, Sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.6	Facility	The Vendor shall 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.	**Sentinel exceeds this requirement.** The Sentinel monitoring center features the following technology for its redundant Internet and telephone communications: ▪ T-1 telephone trunks, provided from three (3) redundant leading providers, to prevent against outages ▪ 432 Fiber-optic telecom cable lines and 200 POTS lines fed directly into the Sentinel facility ▪ Primary provider, Cox Communications (a leading provider of communications) is regionally headquartered within 8 miles and has triple electrical and data redundancy ▪ Second redundant carrier, AT&T ▪ Third redundant carrier, TW Telecom ▪ Cisco IP Telephony Solution combined with Cisco Networking for providing statistical tracking of all data and telephone activity

			A confidential, predefined and rehearsed protocol is set up with Sentinel's telecoms provider to enable a rapid transfer in accordance with the agreed service level. The back-up call handler functions in an active state and is ready to receive calls from the monitoring units as soon as the calls are rerouted from the primary call handler by Sentinel's Telecom providers. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart so it will be unaffected by a manmade or natural event or loss of electrical or communications services that would disable the primary monitoring center. Sentinel's secondary redundant electronic monitoring center is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.7	Facility	The Vendor shall perform complete support of all interface hardware and software equipment (within the monitoring center) necessary to ensure provision of the service for the duration of the contract.	**Sentinel exceeds this requirement.** Support of all interface hardware and software equipment will be provided by Sentinel personnel and equipment through its state-of-the-art monitoring facility located in Irvine California that houses the central computer system and monitoring personnel responsible for supporting the proposed solution. **Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations for the duration of the contract.** **IMPORTANT SENTINEL ADVANTAGE:** To support operations for monitoring center support of all interface hardware and software equipment issues, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP). While Sentinel's primary monitoring center is located in California, its back-up monitoring center is located in Atlanta, Georgia, over 500 miles apart. Sentinel's secondary redundant electronic monitoring center is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup

			monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.8	Facility	The Vendor shall provide the Agency a contact number, accessible twenty (24) hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced.	**Sentinel meets this requirement.** Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center. All monitoring services including receipt of problem reports and problem resolution will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Additionally, Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.**
2.9	Facility	In the event any component of the Vendor's Monitoring Center service becomes inoperable, the Vendor shall immediately notify the Agency Program Manager or designee by telephone or alternate acceptable communication method, but no later than thirty (30) minutes after service failure.	**Sentinel meets this requirement.** In the event any component of Sentinel's monitoring center service becomes inoperable, Sentinel will notify all affected participating agency Program Managers or designees by telephone, no later than 30 minutes after service failure.
2.10	Services	The Vendor's back up Monitoring Center must be activated within 60 minutes of initial system failure or disaster.	**Sentinel meets this requirement.** Sentinel operates two (2) geographically redundant monitoring centers in Irvine, California and Atlanta, Georgia. To support business operations for electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a fully-redundant monitoring center. Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational

			and staffed during normal business hours is capable of being promptly **(within 60 minutes)** staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.11	Services	The Vendor's primary Monitoring Center shall be fully operational and staffed adequately to support the operations of this Contract, twenty four (24) hours a day, 7 days a week, 365 days per year with highly skilled technicians that have completed an initial course of training.	**Sentinel exceeds this requirement.** Sentinel **operates** both its primary monitoring center located in Irvine, California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with highly trained technicians and personnel, from which Sentinel handles over 50,000 calls on a daily basis. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** **IMPORTANT SENTINEL ADVANATGE:** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a monitoring center failure or service catastrophe and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA**

			alcohol electronic monitoring contractor for more than 11 years since the WSCA contract's inception. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's monitoring center is staffed with bilingual personnel on every shift in order to ensure successful interactions with its agency customers. Sentinel monitoring center personnel typically answer 96% of all calls within eight (8) seconds and provide an on-hold wait time of four (4) seconds or less. All of Sentinel's monitoring center employees undergo a thorough and detailed training and certification program, during which they are trained in all aspects of electronic monitoring equipment and software including troubleshooting and the necessary alarm procedures to ensure timely and accurate notifications. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel monitoring center staff is cross-trained to support assistance requests for radio frequency (RF) electronic monitoring, voice verification monitoring programs, **breath alcohol testing (BAT), transdermal alcohol monitoring** and global positioning satellite (GPS) tracking should any participating agency be utilizing more than one (1) service category. Two (2) full weeks are used during the training of a new monitoring center operator to ensure that a thorough electronic monitoring knowledge based is developed. Complete equipment functionality and software platform protocols must be understood prior to graduation to a Level One Monitoring Center Operator. The training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge- and performance-based, allowing maximum participation by monitoring center staff and supervisors. The training techniques, tools, and exams are developed by the training coordinator and are required to successfully complete the certification process. The coordinator will conduct training sessions at regularly scheduled intervals; however, each shift supervisor will be instrumental in the development of their employees. **Monitoring Center On-going Training:** To maintain an efficient service oriented organization, Sentinel employs on-going training modules for all

positions. This method is applied equally to all monitoring center operators as to allow correct interpretation and dissemination of information to all authorized agency personnel. The training modules for each employee within the monitoring center are delineated. Sentinel is committed to providing the highest level of monitoring services in the industry. A critical element of providing reliable and efficient monitoring is a knowledgeable, professional and well-trained staff.

This training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge and performance based, allowing maximum participation by monitoring center staff and supervisors. A grading system has been established to easily identify staff members with certain knowledge and ability. This grading system requires an employee to demonstrate acquired skills through verbal and written examinations.

Levels:

- Monitoring Specialist Level – Trainee
- Monitoring Specialist Level – 1
- Monitoring Specialist Level – 2
- Monitoring Specialist Level – 3
- Monitoring Shift Supervisor

Training / Certification: The Training Coordinator is responsible for developing the training techniques, tools, and exams that are required to successfully complete the certification process. The Training Coordinator will conduct training sessions at regularly scheduled intervals; however each shift supervisor will be instrumental in the development of their employees. Training for the various levels will be conducted as follows:

Level	Training Conducted By	Certified By
Trainee	Training Coordinator	Training Coordinator
1	Shift Supervisor	Training Coordinator
2	Shift Supervisor	Training Coordinator
3	Training Coordinator	Training Coordinator
Shift Supervisor	Monitoring Center Manager	Monitoring Center Manager

Certification Exams: A written examination is prepared for each grade level.

Some grade levels require that an employee demonstrate acquired skills. A minimum test score is required to pass the written examination.

Level	Minimum Score
Trainee	85%
1	85%
2	85%
3 / Shift Supervisor	90%

A passing score is mandatory for the Trainee and Level 1 position and is required for continued employment. The Level 1 certification exam must be successfully completed before the expiration of a new employee's orientation period. Re-testing periods are established to give an employee an additional attempt to achieve a passing score.

Level	Testing Period	Re-Testing Period	Passing Score
Trainee	When initial training complete	14 Days	Mandatory
1	10 weeks' employment	14 Days	Mandatory
2	90 Days	30 Days	Not Mandatory
3	90 Days	30 Days	Not Mandatory

A passing score is mandatory for continued employment beyond the orientation period for the Trainee and Level 1 grade.

Promotion: This performance-based program ensures that qualified candidates are promoted in a manner consistent with Sentinel's goal of maintaining a knowledgeable and professional staff. A staff member will be promoted upon successful completion of the certification process. An employee that meets the length of service requirements for a grade promotion must be recommended for advancement by their supervisor. Supervisors are advised to consider the following items before recommending an employee for promotion.

Performance:

- Attendance
- Dependability

			Measuring Tools: ▪ Report ▪ Charts
2.12	Services	The Vendor must provide a staffed communication system utilizing an 800-telephone number an 800- number fax, and email access, available 24-hours per day, 7 days per week, 365 days per year at no additional charge to the Agency for technical, analysis, and application assistance.	**Sentinel exceeds this requirement. Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile numbers and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center for technical, analysis, and application assistance at no additional charge to the participating agencies.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** **IMPORTANT SENTINEL ADVANTANGE: Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring outsource monitoring services/help desk services to third-party providers for both radio frequency monitoring and alcohol monitoring thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.) **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly **(within 60 minutes)** staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.13	Services	Deleted.	
2.14	Services	The Vendor's Monitoring Center Service	**Sentinel exceeds this requirement.** Staffed customer service operators are

		must be able to provide for offender enrollments and scheduling to be performed via direct telephone request (password accessible) when Agency staff (officer) does not have immediate access to an internet connection.	available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies. **The Sentinel monitoring center is readily accessible toll free by phone (password accessible) process service requests when agency staff (officer) does not have immediate access to an Internet connection.** Sentinel monitoring center operators have the expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, **entering or changing a participant's schedule, performing participant enrollments or entering data into the system**. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. **Each participating agency staff member will be supplied with a unique verbal password which must be provided to the monitoring center operators when calling in to request data modifications.**
2.15	Services	The Vendor's Monitoring Center Service must be able to activate or deactivate Alcohol Monitoring services for an offender within 30 minutes after receipt of request by fax, telephone or e-mail notification from an the Officer.	**Sentinel exceeds this requirement.** Staffed customer service operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies. **Sentinel will process all requests to enroll or deactivate alcohol monitoring services for an offender within 30 minutes after receipt of request by fax, telephone or e-mail notification from an officer.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.16	Services	The Vendor's Monitoring Center service must maintain accurate and concise historical logs of all telephone, text message, emails and fax calls attempted and completed, including date, time, and the associated incident. The Vendor shall make these logs available to the Agency upon request.	**Sentinel exceeds this requirement.** All telephone calls to and from the monitoring center are recorded for training and auditing purposes and are available for later playback. Additionally, the central computer systems continuously receive and retain all monitoring data received, text messages, emails and fax calls attempted and completed, including date, time, and the associated incident. Sentinel will make all agency specific logs available to any WSCA participating agency upon request.
2.17	Services	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 Agency	**Sentinel meets this requirement.** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately 24 hours a day, seven (7) days a week to designated participating agency staff. Sentinel supports all standard methods of

		staff when an alert notification is generated. The Vendor's monitoring service shall include the capability to administer a phone call by a live staff person in the Monitoring Center in response to designated priority alert notifications, at an additional fee.	notification, such page (alpha or numeric), electronic mail, fax, and/or text message to a cell phone. Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. For example, an agency may choose to outline three (3) notification profiles: ▪ **Level 1:** The user will receive event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 2:** The user will receive all tamper and curfew violations immediately by email and/or text message, all event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 3:** The user will receive all event notifications and alert violations immediately by email, text message, and/or manual voice message, and have access to view all participant event and alert information immediately through the software. Please note that the notification levels previously described are examples only. Each agency will have the capability to determine an agency specific level or levels of notification. In addition to automated notifications, Sentinel can offer triage via monitoring center staff where live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage before the system generates

			notification should the agency request this service on an optional price plan.
2.18	Services	The Vendor's Monitoring Center service must triage alerts, including triaging and responding to alerts with direct contact to both Agency staff and offenders for resolution as defined by the Agency. The Monitoring Center service must have the ability to escalate an alert notification if the officer does not acknowledge the notification within an Agency-specified time to the next Agency designated contact. In the event an alert notification is unresolved, the Vendor's Monitoring Center service shall be responsible for contacting the Agency's designated officer via, text message, fax, email or phone. The means or mode of contact shall be at the Agency's discretion. These services shall be provided twenty-four (24) hours 7 days a week.	**Sentinel exceeds this requirement.** In addition to automated notifications, Sentinel can offer triage via monitoring center staff 24 hours a day, seven (7) days a week where live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage before the system generates notification should the agency request this service on an optional price plan. Sentinel will be responsible for maintaining a call tree that will be utilized when contacting participating staff to report alarm notifications pursuant to established protocols. Sentinel understands that if an acknowledgment by one of the participating agency staff members is not made or received within a specified time frame, the alarm notification shall be automatically returned to the monitoring center system, and the call tree escalation process shall be implemented. **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel operates a highly unique automated system via toll-free 800 number for officers to call in and acknowledge receipt of an alert through the Automated Messaging System (AMS). The AMS enables officers secure use of touch tones to rapidly acknowledge receipt of an alert and stop on-going escalation. The AMS also allows offices to immediately connect to a live monitoring center operator or, as always, officers who prefer to clear alerts via voice telephone call with a live operator may call Sentinel's monitoring center direct and toll free 24 hours a day, seven (7) days a week to do so as an alternative to the AMS. Sentinel's

			AMS is complemented by web-based audit capabilities capable of tracking the performance of both Sentinel and the agency's staff/program regarding notification steps and response for each alert. Sentinel's software provides management information reports capable of querying the details related to alert response. Authorized users can perform web-based report queries on any alert(s) to determine: the number of notification steps taken, the contact(s) and method(s) used to attempt notification and the individual who ultimately confirmed receipt of notification – each accompanied by the date/time of occurrence. This unique Sentinel capability provides unparalleled accountability for user agencies. **IMPORTANT SENTINEL ADVANTAGE:** Unlike other vendors, Sentinel's proposed solution allows for automated acknowledgement AND automated escalation procedures. As this is completed through the software, this eliminates the possibility for human error therefore creating a more accurate and reliable system of escalation.
2.19	Services	The Vendor's Monitoring Center service must provide the capability for every human voice call in and out of the system to be recorded with a transaction record that indicates the called number or calling number, and the result of the call. This information shall be made available to the Agency Program Manager at the Agency's request.	**Sentinel exceeds this requirement.** All telephone calls to and from the monitoring center are recorded for training and auditing purposes **and are available for later playback**. Sentinel tracks **all** transaction records indicating the called number or calling number, and the result of the call. Sentinel will make this information available to the respective participating agency Program Manager upon request.
2.20	Services	The Vendor's Monitoring Center must provide an initial response to pre-determined alert notifications to troubleshoot and resolve the notifications per established protocols.	**Sentinel exceeds this requirement.** Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage before the system generates notification to perform initial troubleshooting and resolution of pre-determined notifications should the agency request this service. In addition to automated notifications, Sentinel can offer triage via monitoring

			center staff where live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record.
2.21	Services	The Vendor's Monitoring Center service must be able to tailor the level of alert notification to the Agency or individual needs or protocols.	**Sentinel meets this requirement.** Sentinel's monitoring service can tailor the level of alert notification to meet individual agency needs and protocols, including but not limited to all aspects of notification defined by this WSCA RFP. Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. For example, an agency may choose to outline three (3) notification profiles: ▪ **Level 1:** The user will receive event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 2:** The user will receive all tamper and curfew violations immediately by email and/or text message, all event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 3:** The user will receive all event notifications and alert violations immediately by email, text message, and/or manual voice message, and have access to view all participant event and alert information immediately through the software.

			Please note that the notification levels previously described are examples only. Each agency will have the capability to determine an agency specific level or levels of notification. **IMPORTANT SENTINEL ADVANTANGE:** Sentinel **monitoring services are** ISO 9001:2008 certified and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations **including agency/departmental specific operational procedures for monitoring and notification protocols.** **IMPORTANT SENTINEL ADVANTAGE:** Each agency user will have the capability through the respective alcohol monitoring software to customize alert notification profiles on a per participant basis should the agency/user decide to utilize this feature. Each authorized user within the agency will then have the ability to choose from the agency-determined notification protocols on a per participant basis. For example, an officer can choose to receive only an email notification of test refusal violations for a particular participant on remote breath alcohol monitoring but may choose to receive a telephone call and an emailed report of the violation for a different participant on either breath alcohol or transdermal alcohol monitoring. Additionally, individual users can choose to exclude certain events from notification if deemed unnecessary on a per participant basis. These events would still be included on daily, weekly or monthly reports. Notification methods can also vary by supervising personnel.
2.22	Services	The Vendor's Monitoring Center must be responsible to maintain a call tree to be utilized when contacting Agency staff to report alert notifications pursuant to established protocols and optional price plan.	**Sentinel exceeds this requirement.** Sentinel will be responsible for maintaining a call tree that will be utilized when contacting participating agency staff to report alarm notifications pursuant to established protocols. Sentinel understands that if an acknowledgment by one of the participating agency staff members is not made or received within a specified time frame, the alarm notification shall be automatically returned to the monitoring center system, and the call tree escalation process shall be implemented. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel operates a highly unique automated system via toll-free 800 number for officers to call in and acknowledge receipt of an alert through the Automated Messaging System (AMS). The AMS enables officers secure use of touch tones to rapidly acknowledge receipt of an alert and stop on-going escalation. The AMS also allows offices to immediately connect to a live monitoring center operator or, as always, officers who prefer to clear alerts via voice telephone call with a live operator may call Sentinel's monitoring center direct and toll free 24 hours a

			day, seven (7) days a week to do so as an alternative to the AMS. Sentinel's AMS is complemented by web-based audit capabilities capable of tracking the performance of both Sentinel and the agency's staff/program regarding notification steps and response for each alert. Sentinel's software provides management information reports capable of querying the details related to alert response. Authorized users can perform web-based report queries on any alert(s) to determine: the number of notification steps taken, the contact(s) and method(s) used to attempt notification and the individual who ultimately confirmed receipt of notification – each accompanied by the date/time of occurrence. This unique Sentinel capability provides unparalleled accountability for user agencies. **IMPORTANT SENTINEL ADVANTAGE:** Unlike other vendors, Sentinel's proposed solution allows for automated acknowledgement AND automated escalation procedures. As this is completed through the software, this eliminates the possibility for human error therefore creating a more accurate and reliable system of escalation. **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record.
2.23	Services	In the event of an alert violation, the Monitoring Center service must provide to the Officer, at a minimum the Offender's name, type of violation, time of violation.	**Sentinel meets this requirement.** Alert notifications sent to department staff will include, at a minimum, the program participant's name, the nature / type of the alert, the date and time of the alert, and notes or actions (other info), if any, taken by Sentinel staff.
2.24	Services	The Vendor's Monitoring Center service must be able to tailor the level of alert notification to the Agency or individual needs or protocols at an optional price plan.	**Sentinel meets this requirement.** Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. For example, an agency may choose to outline three (3) notification profiles: ▪ **Level 1:** The user will receive event notifications and alert violations

			in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 2:** The user will receive all tamper and curfew violations immediately by email and/or text message, all event notifications and alert violations in a daily summary and have access to view all participant event and alert information immediately through the software. ▪ **Level 3:** The user will receive all event notifications and alert violations immediately by email, text message, and/or manual voice message, and have access to view all participant event and alert information immediately through the software. **Please note that the notification levels previously described are examples only. Each agency will have the capability to determine an agency specific level or levels of notification.** Sentinel is ISO 9001:2008 certified and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations **including agency/departmental specific operational procedures for monitoring and notification protocols.** At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage before the system generates notification to perform initial troubleshooting and resolution of pre-determined notifications should the agency request this service on an optional price plan.
3.0.	**SECTION C Data Center, Data Storage, and Data Access**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
3.1	Data Center	The facility housing the Data Center(s) must have multiple physical security features. Describe the physical security features that protect the Data Center and agency data.	**Sentinel meets this requirement.** The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the data centers utilized to support the remote alcohol monitoring solution. **Additionally, this is the central location from which all monitoring center activities are conducted and information is disseminated.** All transdermal alcohol monitoring data is separately managed, run, and serviced through SAS 70 audited data centers in two (2) distinct locations ViaWest in Centennial and Qwest Cyber Center in Colorado. **Physical Security of Remote Alcohol Monitoring Facilities:** The

			continuously staffed Sentinel monitoring centers reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center

			are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified. **Physical Security of Transdermal Alcohol Monitoring Facilities:** The transdermal alcohol monitoring data centers are secured so that access is restricted to authorized individuals. Visitors must press a buzzer to contact the receptionist, who can see the individual on the door camera and the building camera before admitting the individual into the main lobby. Visitors must sign a log, and are then issued a visitor badge that must be displayed at all times. They must be escorted at all times while visiting the facility. All visitors must sign out and surrender their visitor's badge when they leave. Internal security is maintained through the use of electronic door controls, accessed through security proximity cards, which access schedules of when employees are allowed to be in the building. The building is under camera surveillance at all times. Outside lighting on the perimeter of the building illuminates both the building and the parking lots adjacent to the building. The parking lot perimeter is also monitored by a closed circuit infrared/low light TV system. Cameras are strategically placed in the lobbies and in the elevators, and all transmissions are both monitored and recorded twenty-four hours a day. **Security of Monitoring Records:** In Sentinel's experience with offender populations nationwide, Sentinel understands the importance of data integrity

			both in its actual data entry as well as its subsequent data retention. To ensure that the proper information is entered at all times, Sentinel's personnel are thoroughly trained on data entry procedures with supervisorial support for any adjustments or corrections. Each user is given their own login and once they set their confidential password Sentinel can ensure the integrity of each user's entry. This unique user access allows Sentinel's Information Technology personnel to follow electronic audit trails that allow supervisors and management to verify the source of all date entry. All remote alcohol monitoring data is actually stored on Sentinel's central servers located in its secure corporate facility. The workstations that Sentinel's staff and agency personnel use at local facilities are technically only used to connect to Sentinel's central server. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. In addition, Sentinel's monitoring center, data centers and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Any instance of failure resulting in a loss of monitoring capability will be reported to the participating agency. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. All of Sentinel's security systems are monitored continuously.

			Monitoring System Security: Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. To prevent unauthorized access from outside the monitoring and/or center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platforms use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.

3.2	Data Center	The Vendor's Data Centers should have ventilation and temperature control adequate to ensure proper functions of the Monitoring Center hardware.	**Sentinel meets this requirement.** The primary monitoring center is a separate, self-supporting node within the facility that is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. The continuously staffed Sentinel monitoring center houses the data center for remote alcohol monitoring and resides in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community. Additionally, all transdermal alcohol monitoring data is separately managed, run, and serviced through SAS 70 audited data centers in two (2) distinct locations. These two data centers are based on different networks, power grids, central offices and service providers. Each data center has redundancy for all areas including cooling, ventilation, electrical, power generation and telecommunications to ensure proper functions of the data center hardware.
3.3	Data Center	The Vendor's Data Centers must have back-up emergency power generators.	**Sentinel exceeds this requirement.** The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the primary data centers utilized to support the remote alcohol monitoring solution. Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-the-art technology including: ▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator. Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS

			unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's on-site diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. **Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled.** The diesel generator is regularly inspected to ensure that it remains in operational order at all times. Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days. Sentinel will institute fail-over procedures should any continuous commercial power outages occur that jeopardizes participant monitoring. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers which can be utilized to support the remote alcohol monitoring solution are located in Atlanta, Georgia, over 500 miles apart. To support operations for database replication of key IT and failover disaster recovery, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers at a state-of-the-art, fully-secured facility that has both redundant short-term and long-term power supplies. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full on-site and full off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. All transdermal alcohol monitoring data is separately managed, run, and serviced through SAS 70 audited data centers in two (2) distinct locations.

			These two data centers are based on different networks, power grids, central offices and service providers. If commercial AC power is lost to either transdermal alcohol monitoring data center. uninterruptible power supplies (UPS) instantly deliver backup power to all servers and buildings for up to 30 minutes. For the data center areas, a diesel-powered generator comes online within six (6) seconds. The generator delivers power to the entire building for up to one (1) week, with diesel fuel deliveries scheduled weekly thereafter. **Sentinel has never lost any data or performance capability due to power losses of any sort.**
3.4	Data Center	The Vendor must have redundant Data Centers 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 Data Center.	**Sentinel exceeds this requirement.** To support business operations for database replication of key IT, and failover disaster recovery, Sentinel's monitoring system incorporates redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and redundant DRP servers which can be utilized to support the remote alcohol monitoring solution are located in Atlanta, Georgia, **over 500 miles apart**. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full on-site and full off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a manmade or natural event the causes major disruption to electrical or communications services to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. All transdermal alcohol monitoring data is separately managed, run, and serviced through SAS 70 audited data centers in two (2) distinct locations ViaWest in Centennial and Qwest Cyber Center in Colorado. These two data centers are based on different networks, power grids, central offices and service providers that are located sufficiently distant, 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 data center.. Each data center has redundancy for all areas including cooling, ventilation, electrical, power generation and telecommunications to ensure proper functions of the

			data center hardware.
3.5	Data Center	All back-up systems in the Data Centers must be tested regularly.	**Sentinel exceeds this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing its monitoring centers, all of the proposed systems data centers and the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel customizes its Risk Mitigation and Disaster Recovery Plan to each agency upon contract award and will provide this plan to any requesting agency post award. All revisions/updates to this plan will be forwarded to the agency as they occur. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. **Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.** **IMPORTANT SENTINEL ADVANTAGE:** A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure, the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. Additionally, the transdermal alcohol monitoring system incorporates a Business Continuity Plan with the supporting infrastructure in the area of data back-up and recovery, in order to prevent business interruptions. This plan includes data protection, risk assessment information, infrastructure security, back-up and recovery processes, as well as performance monitoring practices. It ensures the protection of critical assets and customer data. All of Sentinel's proposed security systems are monitored continuously.
3.6	Data Center	The Vendor's system should provide for 100% redundancy to avoid unnecessarily	**Sentinel exceeds this requirement.** Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that serves to

		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.	immediately protect all computers and electronic equipment from downtime continuing to power the entire monitoring center as normal and can do so while Sentinel's on-site diesel generator automatically begins operation. Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs on all monitoring solutions while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. **Regardless of the cause, Sentinel's contingency plans will failover in the case of any system malfunction that effects participant monitoring or reporting, which cannot be corrected within one (1) hour.** To support operations for database replication of key IT, and failover disaster recovery to avoid unnecessarily excessive downtime due to hardware or software issues, Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers which can be utilized to support the remote alcohol monitoring solution are located in Atlanta, Georgia, over 500 miles apart. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. Redundant web servers, application servers and database servers, are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. Sentinel uses an industry standard data protection and recovery software

			package to ensure that the databases within the primary and back-up data servers are concurrently maintained, which ensures the following: ▪ No loss of data from the databases if there is a failover ▪ Capability for the back-up database to immediately and automatically become available for processing and access The system maintains a constant connection between the primary and back-up database servers and when it detects the loss of a regular "heartbeat" signal between the systems, it automatically initiates an alert notifying Sentinel of this loss. It is then determined if the loss of heartbeat was an anomaly or it is warrants a real-time failover from the primary database server to the back-up server. All transdermal alcohol monitoring data is separately managed, run, and serviced through SAS 70 audited data centers in two (2) distinct locations ViaWest in Centennial and Qwest Cyber Center. These two data centers are based on different networks, power grids, central offices and service providers. Each data center has redundancy for all areas including cooling, ventilation, electrical, power generation and telecommunications to ensure proper functions of the data center hardware. Additionally, the database hardware is a clustered group of nodes (on two servers, rather than a single server). Any one of the nodes can handle the full workload of the database needs and features a database test restore server that can be used as a production replacement in the event of a catastrophic failure. The transdermal alcohol monitoring web servers are a group of nodes (seven servers, rather than just a single server), which provide for load balancing and the communications servers are a group of nodes (ten servers, rather than just a single server), which provide for load balancing with multiple telecom carriers. If a server in a work group (database, web, or communications) fails, the transdermal alcohol monitoring current redundancy levels in the work groups ensure that Sentinel customers will not see or experience the failure through a formal Business Continuity Plan with the supporting infrastructure in the area of data back-up and recovery, in order to prevent business interruptions. This plan includes data protection, risk assessment information, infrastructure security, back-up and recovery processes, as well as performance monitoring practices. It ensures the protection of critical assets and customer data. Additionally, to ensure availability of all data, the plan call for the replication of all data daily to online storage arrays at three (30 separate geographic locations. The database is tested

			daily to ensure system backup can be used on recovery of any system. In addition, the plan calls for a data "snapshot" every four (4) hours to maintain backups. Transaction logs for all activity ensure that a data restore will be complete, and that each transaction is available.
3.7	Data Storage	The Vendor must ensure that all records (automated or hard copy files) remain the property of the Agency and shall be returned within 30 days, in the event the contract is canceled or terminated.	**Sentinel meets this requirement.** All records created for participants referred to this program by any participating agency will remain solely the property of the participating agency. Upon completion of services, all records (automated or hard copy files) will be returned to the participating agency within 30 days or destroyed under direction of agency staff.
3.8	Data Storage	The Vendor's system must ensure that all data be recorded with a historical transaction record and stored/archived for retrieval/backup in a database when requested by Agency personnel in accordance with the following:	**Sentinel meets this requirement.** Both the remote alcohol and transdermal alcohol computer software system databases immediately and automatically (in real-time) record with a historical transaction records all of the data received by the monitoring equipment, entered at the time of enrollment, data and/or monitoring changes, monitoring reports and terminations exchanged between officers and the monitoring center facility. Additionally, the system databases store/archive for retrieval/backup all monitoring data so that all authorized users can view or exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure access.
3.9	Data Storage	a. All historical data must be centrally stored and accessible for reporting purposes;	**Sentinel meets this requirement.** The MEMS 3000 software system database stores/archives for retrieval/backup all monitoring data so that all authorized users can view or exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure access. When data is received from SCRAMx, it is centrally stored in ScramNET, the web-based application, where offender data is collected, analyzed, and maintained in a secure, central location. This central information hub houses all offender data and allows courts and supervising agencies to access and manage their data from any web-based browser.
3.10	Data Storage	b. This information must be available for reporting in a standard transaction file format; and	**Sentinel meets this requirement.** Authorized users have the ability to directly access all participant historical information through Sentinel's remote alcohol computer software system database or ScramNET. All monitoring reports are available through the proposed software's easy-to-use report generator applications in a standard transaction file format.
3.11	Data Storage	c. All current and historical data files must be retained for a minimum period of seven (7) years and this information shall be available at no charge to the Agency.	**Sentinel exceeds this requirement.** Sentinel secures all remote alcohol monitoring system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. Databases are backed up on removable discs, using the industry recognized Symantec

			Backup Exec software data back-up and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel. If system recovery is necessary, Sentinel is not limited to the sole use of back-ups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler. Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups. The proposed transdermal alcohol monitoring data center is also equipped with multiple computers. In addition, a full mirror of the central database is maintained, which is approximately five (5) seconds behind the production database with full replication and data journaling in a near real-time mode. The following data backups are employed: ▪ Complete backups are performed every night. ▪ Backups are copied to online SANs (Storage Array Networks) in two (2) separate data centers. ▪ Backups are tested every night by restoring the backup to a secondary database server, then running reports to ensure the backup is complete. The configuration of this secondary server is similar to production database nodes, hence this server can be pressed into service as a production replacement in the unlikely event of a catastrophic failure. The server ensures that data from the previous day's backup are restored and running as of 4:00 am each morning. ▪ Backups are kept online (not on tape) for faster restores and prompt availability. ▪ Five years' worth of backups are stored online and all monitoring data will be **retained off-line indefinitely ensuring a minimum period of seven (7) years.**
3.12	Data Storage	The Vendor's Data Centers must have	**Sentinel exceeds this requirement.** The workstations within Sentinel's

		duplicate computers with the ability to, at a minimum, permit restoration of data collection and user monitoring services within 10 minutes after computer failure. The Monitoring Center should have duplicate data storage devices with automated fail-over and automatic re-establishment of the duplicate databases upon replacement of the failed storage device.	monitoring centers are equipped with redundant features; all of the computer systems in Sentinel's monitoring centers are designed to perform the same monitoring functions. They are all "ghosted" or duplicate workstations that process the incoming signals similarly. If one of the computers is not functioning properly, all incoming signals are simply routed **immediately** to one of the other available computers. In addition, Sentinel employs internal Information Technology personnel based here at the same facility. In the event that a computer, facsimile or modem error occurs, Sentinel's IT personnel quickly replace the computer component with no affect on the alarm processing capabilities of the entire system. Along with spare computer workstations, Sentinel has additional equipment available to replace facsimile machines, modems and all other monitoring center components thus allowing seamless operation of the monitoring center at all times. Sentinel secures all system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. Databases are backed up on removable discs, using the industry recognized Symantec Backup Exec software data back-up and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure l fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel. **If system recovery is necessary, Sentinel is not limited to the sole use of back-ups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler.** Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups. The proposed transdermal alcohol monitoring data center is also equipped with multiple computers. In addition, a full mirror of the central database is

			maintained, which is approximately five (5) seconds behind the production database with full replication and data journaling in a near real-time mode. The following data backups are employed: ▪ Complete backups are performed every night. ▪ Backups are copied to online SANs (Storage Array Networks) in two (2) separate data centers. ▪ Backups are tested every night by restoring the backup to a secondary database server, then running reports to ensure the backup is complete. The configuration of this secondary server is similar to production database nodes, hence this server can be pressed into service as a production replacement in the unlikely event of a catastrophic failure. The server ensures that data from the previous day's backup are restored and running as of 4:00 am each morning. ▪ Backups are kept online (not on tape) for faster restores and prompt availability. ▪ Five years' worth of backups are stored online and all monitoring data will be **retained off-line for a minimum period of seven (7) years.**
3.13	Data Storage	Upon request from the Agency, 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 to be determined by the Agency.	**Sentinel meets this requirement.** Upon request, Sentinel will provide the most up-to-date complete copy of the respective agencies monitoring data included in 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 the participating agency and in a manner that will not compromise overall confidentiality and system integrity.
3.14	Data Access	The Vendor shall 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-Agency personnel, without prior written approval from the Agency Program Manager.	**Sentinel meets this requirement.** At no time will Sentinel ever disclose confidential data including 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 any unauthorized personnel without written approval of the participating agency Program Manager. All program data will be maintained in accordance with secure data protection standards. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services,

			all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.15	Data Access	The Vendor must maintain unaltered recorded data of offender violations, to be accessible in original form and substance for utilization as physical evidence for prosecution.	**Sentinel exceeds this requirement.** The remote alcohol computer software system database maintains unaltered recorded data of offender violations, accessible in their original form and substance for utilization as physical evidence for prosecution. Sentinel tracks **all** changes to the application, including but not limited to participant or agency details, notes, alert resolutions, enrollments, terminations and service requests. When data is received from SCRAMx, it is stored in ScramNET, the web-based application, where offender data is collected, analyzed, and maintained in a secure, central location. ScramNET will notify the supervising authority of any alcohol readings, tamper alerts, or equipment malfunctions, so that appropriate action can be taken. This central information hub not only houses all offender transdermal alcohol monitoring data, but allows courts and supervising agencies to access and manage their data, accessible in their original form and substance for utilization as physical evidence for prosecution, from any web-based browser. **IMPORTANT SENTINEL ADVANTAGE:** SCRAMx has an unrivaled record of court admissibility and peer-reviewed research when compared to any other CAM system on the market.
3.16	Security	The Vendor shall have documented policies and procedures for network security, application security, data transmission and data security, as well as Monitoring Center physical security.	**Sentinel exceeds this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan for all of the proposed system's data centers. This plan includes documented policies and procedures for network security, application security, data transmission and data security, as well as monitoring/data center physical security. Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. **Network and Data Transmission Security:** To prevent unauthorized access from outside the monitoring and/or data center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed

			monitoring platforms use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Application Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The proposed systems have the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. **Data Security:** Sentinel's monitoring center, data centers and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel/intrusion. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating

			agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **Physical Security of Remote Alcohol Monitoring Facilities:** The continuously staffed Sentinel monitoring centers reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's

			Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified. **Physical Security of Transdermal Alcohol Monitoring Facilities:** The transdermal alcohol monitoring data centers are secured so that access is restricted to authorized individuals. Visitors must press a buzzer to contact the receptionist, who can see the individual on the door camera and the building camera before admitting the individual into the main lobby. Visitors must sign a log, and are then issued a visitor badge that must be displayed at all times. They must be escorted at all times while visiting the facility. All visitors must sign out and surrender their visitor's badge when they leave. Internal security is maintained through the use of electronic door controls, accessed through security proximity cards, which access schedules of when employees are allowed to be in the building. The building is under camera surveillance at all times.

			Outside lighting on the perimeter of the building illuminates both the building and the parking lots adjacent to the building. The parking lot perimeter is also monitored by a closed circuit infrared/low light TV system. Cameras are strategically placed in the lobbies and in the elevators, and all transmissions are both monitored and recorded twenty-four hours a day.
3.17	Security	The system shall provide security features, which prevent unauthorized individuals from accessing any information held by the Vendor. Secure access to the system shall be maintained at all times.	**Sentinel meets this requirement.** **Monitoring System Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The systems have the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. To prevent unauthorized access from outside the monitoring and/or data centers, the proposed software systems use leading Internet security features, including 128-bit encryption, firewalls and intrusion detections systems. Both the proposed monitoring platforms use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** Sentinel's remote alcohol monitoring system is only accessible via a Cisco ASA firewall blocking any unauthorized access form the Internet to ensure the remote connection is not compromised. **Personnel Security:** **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of

			these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.18	Security	The Vendor must maintain security policies and procedures for its network security, application security, data transmission security, data storage security, and physical security. While it is not necessary for the vendor to submit these documents with proposal, they must be provided to any requesting agency post award.	**Sentinel exceeds this requirement.** Sentinel has provided an overview of its security policies and procedures for network security, application security, data transmission security, data storage security and physical security in response to the specification 3.16 in the section of its proposal. Sentinel maintains security policies with its Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, Monitoring Center physical security as well as its plan to maintain continuous operations in the event of power failures, telephone system failures, local equipment failures, flood or fire at the monitoring center and data Centers. This plan includes documented policies and procedures for network security, application security, data transmission and data security, as well as monitoring/data center physical security. Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. Post award upon request, Sentinel will supply a requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
3.19	Security	The Vendor shall provide secure transmission and storage of data and must ensure that all data, data transmissions and data storage is kept confidential.	**Sentinel meets this requirement.** Sentinel provides secure transmission and storage of all monitoring data and has policies and procedures in place to ensure that all data, data transmissions and data storage is kept confidential. **Network and Data Transmission Security:** To prevent unauthorized access from outside the monitoring and/or data center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed

			monitoring platforms use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Application Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The proposed systems have the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. **Data Security:** Sentinel's monitoring center, data centers and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel/intrusion. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating

			agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.20	Security	The Vendor's facility, equipment, data transmissions, and data storage shall be secure. The Vendor's facility shall be alerted and monitored by a local law enforcement Agency or security company. The alert line shall be a tamper-resistant dedicated circuit and shall not be exposed to any person or	**Sentinel meets this requirement.** Sentinel has provided an overview of its security policies and procedures for network security, application security, data transmission security, data storage security and physical security in response to the specification 3.16 in the section of its proposal. Sentinel uses multiple security systems including active video/audio systems, alarms system and motion and fire detectors that are monitored by an outside security contractor for supervising the entryways into the facility. The outside security contractor will alert Sentinel each time there is a potential security threat through a

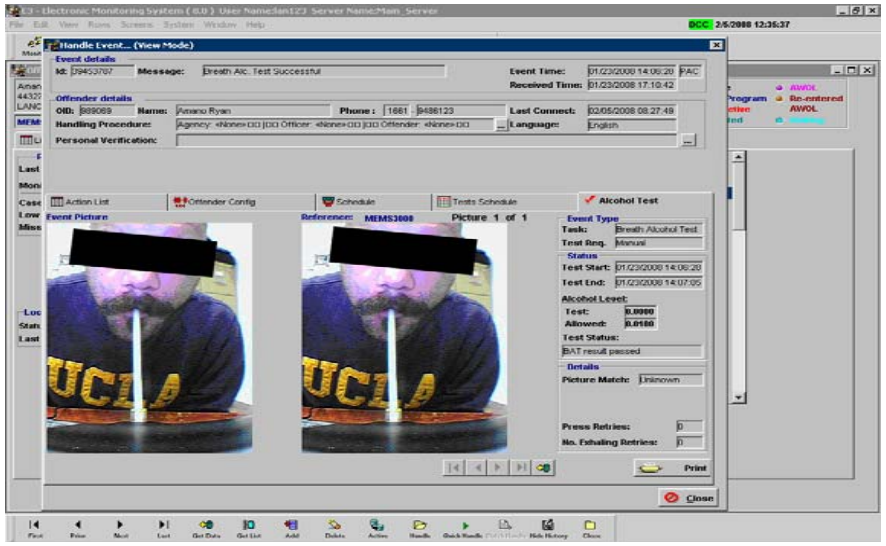
		thing that could alter or damage the line. The Monitoring Center shall be equipped with automated fire detection and suppression equipment.	tamper-resistant dedicated circuit that is secured against any person or thing that could alter or damage the line. The continuously staffed Sentinel monitoring center resides in an independently secured, facility with raised floors, a fire detection and suppression system and written policies and procedures for access that meet all applicable federal, state and local regulations regarding safety. Additionally, Automated fire detection and suppression equipment is standard throughout both data center facilities. The fire detection system monitors for excessive heat, ionization and smoke particulates both above and below the raised floors. All systems are tested at a minimum once per month with maintenance windows to ensure proper operation.
3.21	Security	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.	**Sentinel meets this requirement.** Sentinel has a maintains and routinely tests its comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, monitoring center physical security for each of the proposed solutions as well as its plan to maintain continuous operations in the event of power failures, telephone system failures, local equipment failures, flood or fire at the monitoring center and/or data centers (Please note: Each of these items have been fully addressed previously in this section). Post award and upon request, Sentinel will supply an requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
4a.0	**SECTION D ALCOHOL MONITORING EQUIPMENT AND SERVICE** **Equipment Requirements – for home based receiver**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
4a.1	Equipment	Vendor is bidding the following alcohol monitoring device and the accessories identified in the Price Worksheets. The responses to these specifications are for this equipment. **Alcohol Monitoring Equipment** (Receiver (Home Unit) - Landline) For Product Bid: Mfg.:	**Sentinel meets this requirement.** **Alcohol Monitoring Equipment** (Receiver (Home Unit) - Landline) For Product Bid: Mfg.: 3M Electronic Monitoring Brand/Model: MEMS3000 (also known as 3M Remote Alcohol Monitoring System) **And**

		_____ Brand/Model: _____ **And** **Alcohol Monitoring Equipment** (Receiver (Home Unit) - Cellular) For Product Bid: Mfg.: _____ Brand/Model: _____	**Alcohol Monitoring Equipment** (Receiver (Home Unit) - Cellular) For Product Bid: Mfg.: 3M Electronic Monitoring Brand/Model: MEMS3000 Cellular (also known as 3M Remote Alcohol Monitoring System) Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. **IMPORTANT SENTINEL ADVANTAGE: Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! !
4a.2	Equipment	The Vendor shall provide, at their own expense, all systems and equipment (software and hardware) required for the service delivery, regardless of the actual number of units including but not limited to:	Sentinel meets this requirement. Sentinel is pleased to offer all systems and equipment (software and hardware) required for the service delivery of the MEMS3000 remote breath alcohol testing unit at no additional cost regardless of the actual number of units. The MEMS 3000 is the latest generation in remote Breath Alcohol Testing (BAT) equipment. The MEMS3000 allows Sentinel to remotely monitor participants' breath alcohol levels, as an independent measure or in combination with a restrictive home detention schedule. MEMS3000 remote breath alcohol testing capability enables monitoring of extensive caseloads with high availability and accuracy on one hand while easing the burden on scarce human resources on the other. The following list highlights some of the unique features of the proposed MEMS 3000 alcohol monitoring solution: The MEMS 3000 is a remote alcohol monitoring device that measures the tested individual's breath-alcohol level, similar to the portable systems used by law enforcement.

			▪ Flexible Scheduling Options: The equipment is flexible enough to test participants 24 hours a day, seven (7) days a week by computer generated random tests, monitoring center, agency or officer scheduled testing and on-demand calls to the participant's location. ▪ Landline or Cellular Capability: The optional MEMS3000 Cellular unit enables remote monitoring over cellular networks and accommodates digital lines. When cellular communication is deployed, operators can use the cost efficient GSM and GPRS mode. ▪ Deep Lung Sampling: Intoxilyzer S-D5 alcohol-testing designed to take a deep-lung sample and identify the participant's level of intoxication within a detection range of 0.000 to 0.400 Blood Alcohol Content (BAC). ▪ Court Approved: The equipment provides fuel cell breath alcohol testing through a fixed, secured mouthpiece providing accurate BAC results that are each automatically date and time stamped. ▪ Visual Verification of Participant Identity: The system utilizes automatic lighting sensors, strong flash light that will enable a good resolution capture even in near dark environments, full color images (including test results) and the latest in facial recognition technology for participant identification. ▪ Integration Capability: The MEMS 3000 can be coupled with either radio frequency house arrest monitoring or GPS tracking.
4a.3	Equipment	a. A system with a database to monitor offender testing and communication of data to the Vendor's system;	**Sentinel meets this requirement.** Sentinel will provide each WSCA participating agency, at no additional cost, direct access to the MEMS monitoring database software to monitor offender testing and communication of data, regardless of the actual number of units utilized through this contract.
4a.4	Equipment	b. All software and hardware required to access the Internet, with the exception of Agency personal computers; and	**Sentinel meets this requirement.** Sentinel will provide each WSCA participating agency, at no additional cost, with all software and hardware required to access the MEMS monitoring database software, with the exception of agency personal computers, regardless of the actual number of units utilized through this contract.
4a.5	Equipment	c. All labor, materials, equipment, cellular wireless service costs and consumables necessary to perform Alcohol Testing services on an as-needed basis.	**Sentinel meets this requirement.** Sentinel will provide each WSCA participating agency, at no additional cost, all labor, materials, equipment, cellular wireless service communication costs (as a associated with the units performing tests and calling in the monitoring center) and consumables necessary, regardless of the actual number of units utilized through this

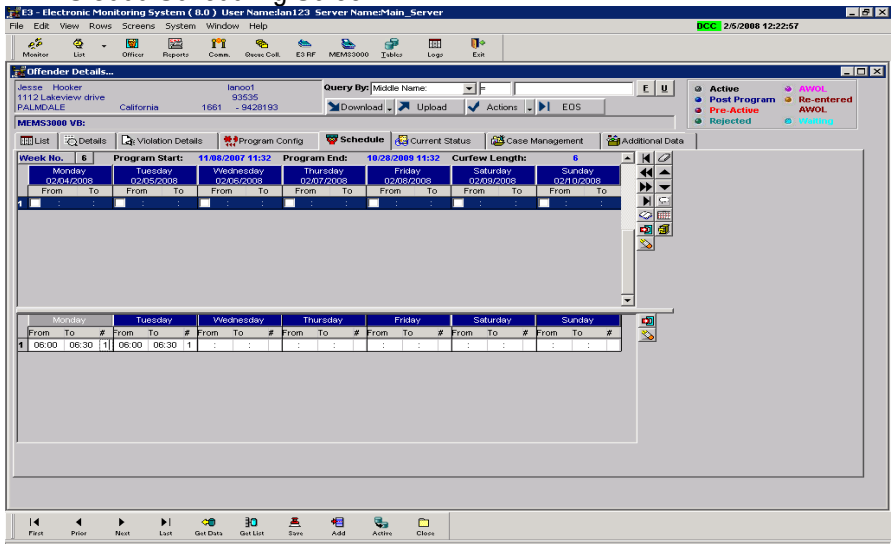
			contract.
4a.6	Equipment	All equipment and systems furnished shall be standard products of the Vendor, shall be in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.	**Sentinel meets this requirement.** The MEMS3000 provides reliable and court-accepted results for breath alcohol testing. Substantially more effective and reliable than alcohol monitoring systems utilizing voice-based participant verification systems, **Sentinel utilizes MEMS3000 units in programs across the United States**. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. **Sentinel employs a Quality Assurance Plan that includes a Final Quality Checklist to the ensure that all initial and new equipment shipment leave the warehouse in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.**
4a.7	Equipment	The Vendor shall provide equipment that meets market safety standards and presents no health or safety hazards to staff and/or offenders.	**Sentinel meets this requirement.** MEMS3000 units are encased in shock resistant plastic and designed to be water, moisture and pest proof. The units do not pose a safety or health threat to agency staff members, the user or the other residents of the household where the device is located.
4a.8	Equipment	The device must be able to either verify the identity of the participant by utilizing a voice or digital imaging recognition system or transmit such data to a monitoring center for participant identification.	**Sentinel exceeds this requirement.** The MEMS3000 alcohol tester is used in conjunction with the camera to a capture picture, identify and confirm the identity of the subject taking the test. An interface circuit combines the camera with the alcohol testing unit allowing the unit to intelligently determine both when to capture the offender's color image and when to send the alcohol level test results. The alcohol testing unit combined with the camera ensures that both the Offender and his/her alcohol level are verified.

			MEMS3000 Visual Identification **IMPORTANT SENTINEL ADVANTAGE:** The unit uses a color picture, visual identification system to verify the identity of the tester during every test (reference MEMS3000 actual images of enrollment image versus test image). The MEMS3000 unit incorporates a strong flash light that will enable a good resolution capture even in near dark environments. The colored jpg picture will be clearly identifiable even in such extreme cases where the background is near darkness. **IMPORTANT SENTINEL ADVANTAGE:** Law enforcement and corrections agencies often prefer visual verification technology over voice verification systems because of the increased difficulty of circumvention. Additionally, the MEMS3000 features a new biometric authentication tool to help monitoring centers confirm the identity of the individual taking the alcohol test. The automated identity verification compares the picture sent with the alcohol test to the one logged in the system as the reference picture, eliminating the need to manually compare results by monitoring center staff. The automatic identity verification tool uses facial recognition technology, which is based on the biometric qualities of the human face. Voice verification is not as reliable as visual verification due to regular, normal and periodic fluctuations in a person's voice that may be caused by illness or time of day (e.g., morning vs. evening, scratchy voice due to cold or flu). Most important, visual verification has proven to be admissible in court, where voice verification has not.
4a.9	Equipment	Instrument must be capable of taking a deep lung sample from the participant's	**Sentinel meets this requirement. The MEMS3000 unit is the latest in random testing technology and captures a deep lung sample via fuel cell**

		breath and compare it to a calibrated breath alcohol standard which may be stored in the system's memory or a supervised test utilizing video imaging solutions	**technology to test for breath alcohol presence.** Breath-alcohol testing is accurate to within + and/or - .005% of actual blood-alcohol levels and is accepted as reliable, court-admissible evidence in numerous courts throughout the nation. There is no need to confirm the tested, measured alcohol consumption with a subsequent urinalysis test. Each completed test is reported to the MEMS3000 monitoring software and compared against a breath alcohol standard stored in the system's memory as shown below (right side of screen). MEMS 3000 Test Results  After receiving indications of a non-compliant test, **the system can provide immediate follow-up testing to confirm the values measured in the initial test(s)**. The agency will dictate the blood-alcohol level that constitutes a violation for participants enrolled in the program.
4a.10	Equipment	The system shall utilize fuel cell or comparable technology, which is specific to alcohol, and shall measure the Breath Alcohol Content (BAC) from the person being tested.	**Sentinel meets this requirement.** The MEMS3000 unit utilizes an Electro-Chemical Breath Alcohol Tester (BAT) providing BAC levels and is highly accurate regarding alcohol consumption assessments by analyzing a deep lung sample and achieving an accuracy rate of +/- 5% relative to the actual alcohol level.

			IMPORTANT SENTINEL ADVANTAGE: The MEMS3000 breath test measures the part-per-million of alcohol present in a deep-lung breath sample. A deep-lung breath sample is obtained by having the participant blow long and hard into the MEMS3000 so that breath from the "bottom" of the participant's lung can be analyzed. Less robust breath testing is inaccurate because mouthwash, after shave lotion, and the like can register as alcohol in the client's system, when in fact, the alcohol is only superficially present. The concentration of alcohol in a deep-lung breath sample (breath alcohol content or BAC) is directly proportional to the alcohol concentration in the blood (blood alcohol content or BAC). Breath-alcohol levels are tested using a fuel cell. Each end of the **fuel cell has two (2) platinum electrodes** that are connected with a wire. When a breath sample is introduced to the fuel cell the platinum causes a chemical reaction that generates an electrical current. The current passes from one end of the fuel cell to the other. A voltage meter measures the strength of the current. When a higher current is measured it indicates higher alcohol content in the participant's breath. The sensor offers standard results common to other police and law enforcement alcohol measuring appliances.
4a.11	Equipment	The system must not respond to natural gas or acetone.	**Sentinel meets this requirement.** The MEMS3000 unit will not respond to natural gas or acetone but instead registers the alcohol found in alcoholic beverages known as ethyl alcohol, also known as ethanol.
4a.12	Equipment	The system shall provide for testing to be conducted at random or fixed intervals that can be set by the Officer on a per participant basis based on the risk of the participant. Describe the number of settings, duration of each interval, the steps involved for an Officer to vary the testing intervals, including but not limited to the steps involved, any time delay or conditions for changes in testing interval to become effective, and whether or not there is a need for monitoring center involvement in varying the testing interval.	**Sentinel meets this requirement. Breath Alcohol Tests can be prompted randomly or at pre-defined fixed intervals that can be set by the officer (no monitoring center involvement required)** on a per participant basis based on the risk of the participant. The agency will have the ability to define the alcohol testing schedules on a per participant basis. For random alcohol testing, officers can define an unlimited number of officer-defined time intervals when the participant can be tested, as well as the number of tests to perform, with a maximum of nine (9) tests per time interval.

MEMS 3000 Scheduling Screen



Officers will also have the ability to edit schedules through the software during a participants monitoring period. Once a schedule has been updated, the unit will completed a download on the next call into the unit in order to initiate that schedule change.

As well as scheduled and/or random fixed interval alcohol tests, monitoring center users can also activate manual on-demand alcohol tests, if and when required. The agency can request the monitoring center initiate an on-demand alcohol test upon any uploaded radio frequency or GPS tracking violation event (as part of the handling procedure).

To alert the participant of the need to take a test, the unit generates a loud audible tone that calls the participant to the unit. At that time the participant presses the “Start” button on the unit and the testing sequence begins. The participant would position themselves in front of the unit facing the camera. He and/or she would then blow into the straw tube attached to the unit and submit the breath sample. The unit informs the participant that the test is complete by visual light diode and the unit transmits the test result to the monitoring system for processing.

4a.13	Equipment	The system may also be capable of testing the client upon entry when it is combined with a Radio Frequency Unit. Describe your available capabilities.	**Sentinel exceeds this requirement. The MEMS3000 can be coupled with either radio frequency house arrest monitoring or GPS tracking or used as a standalone system.** The MEMS3000 equipment can be configured with any alternate tracking/monitoring technology home unit to utilize the same telephone and/or power source. **IMPORTANT SENTINAL ADVANTAGE:** If coupled with alternative tracking/monitoring solutions, agencies can choose to conduct fixed interval alcohol tests in association with the participant's curfew monitoring schedule to perform testing upon entry. Additionally, the agency can schedule an on-demand alcohol test upon any curfew compliance violation events as part of the monitoring center handling procedures.
4a.14	Equipment	Deleted.	
4a.15	Equipment	Tamper detection features on the unit should exist or a supervised test whereby monitoring staff can detect during testing, to ensure the monitoring center receives accurate information on Case alerts and power alerts, and phone alerts.	**Sentinel meets this requirement.** To prevent any unauthorized access to the MEMS3000 testing device, it is factory sealed. The case is fitted with detection components so if a participant tampers with the unit to compromise the case to gain access, a tamper alert is generated. The unit will also monitors for phone and power alerts updating the monitoring center if the phone line is off-the-hook ("Line Busy") or unplugged ("No Answer"). The MEMS3000 also incorporates a tilt detection mechanism to indicate if the participant is attempting to move/relocate the unit to a secondary location. Additionally, the MEMS3000 will register an event when a participant attempts to tamper with the actual testing process. In cases where the participant didn't perform the test when prompted or when the participant didn't conform to the test instructions, the MEMS3000 generates a pre-defined number of test retries (default of 4 retries). The MEMS3000 is capable of transmitting multiple messages that could be related to a participant failing to take the breath-alcohol test to verify Breath Alcohol Content (BAC). The primary messages pertaining to a participant's negligent or intentional failure to take a test are as follows: ▪ **Picture Capture Failed:** Picture not taken due to lack of cooperation from the participant ▪ **Picture Mismatch:** Any person other than the participant has attempted to complete the alcohol test ▪ **BAT Failed - Request Time Out:** The number of test request attempts exceeded the time allotted for one (1) test to be completed successfully ▪ **BAT Failed - Last Retry:** The participant failed due to lack of cooperation; did not blow into straw

			All test results and failures to test are transmitted to and stored at the monitoring center and can be immediately emailed to the supervising officer for use in provoking an admittance or immediate action as a violation. It is important to note that test results are immediate at the time of testing and notifiable to the officer via email, text message or optionally via phone.
4a.16	Equipment	The system must be able to connect to a standard phone line jack or have the ability to also use standard cell phone technology to communicate with the monitoring center and download data.	**Sentinel exceeds this requirement.** The MEMS3000 unit can communicate and download data to the monitoring center over a standard home telephone line, a DSL phone line or through the wireless network. The MEMS3000 cellular unit enables remote monitoring over standard cellular networks and also accommodates digital lines.
4a.17	Equipment	The system shall have the ability to be attached to a radio frequency unit or to be used as a standalone system. Describe how your system is compatible with RF electronic monitoring.	**Sentinel exceeds this requirement. The MEMS3000 can be coupled with either radio frequency house arrest monitoring or GPS tracking or used as a standalone system.** The MEMS3000 equipment can be daisy chained with any alternate tracking/monitoring technology home unit to utilize the same telephone and/or power source. **IMPORTANT SENTINAL ADVANTAGE:** If coupled with alternative tracking/monitoring solutions, agencies can choose to conduct fixed interval alcohol tests in association with the participant's curfew monitoring schedule (upon entry). Additionally, the agency can schedule an on-demand alcohol test upon any curfew compliance violation events as part of the monitoring center handling procedures.
4a.18	Equipment	The device shall be simple to install and have easy to understand instructions.	**Sentinel meets this requirement.** The MEMS 3000 units are small (9" x 10.8" x 12.5") and lightweight (weighs 5.4 pounds) and is easily installed in a participant's home in 10 minutes or less requiring only a home telephone line or cellular signal for communication and **standard 110 AC house current. During installation, officers will need to simply p**lug in the power and plug in the phone line to the unit. Two green lights should appear solid on the back of the unit to confirm proper operation of the unit, power connection and phone line connection.
4a.19	Equipment	The device shall be permanently marked with the model/serial identification numbers and will not change colors or lose labeling after being exposed to common cleaning products. The vendor will replace any device without charge if the tracking number is not legible.	**Sentinel meets this requirement.** Sentinel's MEMS3000 units are equipped with a permanent label that has permanent ink identifying the serial number/model that will not change colors or lose it labeling after being exposed to common cleaning products. Sentinel will replace any device if the equipment tracking number is illegible at no additional cost.
4a.20	Equipment	The device and all additional equipment	**Sentinel meets this requirement.** Sentinel confirms that the MEMS3000 unit

		shall not be available as an open market item if this could compromise the security of the system.	and all its components are not commercially available to the general public or open market items.
4a.21	Equipment	If testing occurs unsupervised by monitoring staff the device may incorporate non-volatile memory capable of storing at least five days worth of events (with date and time of occurrence) at times when the telephone service and electrical power may become unavailable. In particular, non-volatile memory will retain unreported events and report them once power / telephone services have been restored, including date & time of occurrence. As an alternative, a supervised test may be proposed with the capability to detect, reattempt and/or notify on a no answer and/or phone line outage in the area and re-attempt the test/call until successful.	**Sentinel meets this requirement. MEMS3000 results are supervised with the capability to detect, reattempt and/or notify on a no answer and/or phone line outage in the area and re-attempt the call until successful.** The MEMS3000 unit utilizes the "distributed management" concept and therefore has the capability to locally store up to 10 alcohol test schedules to continue testing if communications with the monitoring system are interrupted. The MEMS3000 operates via standard 110 AC house current. In the event of a power outage, the MEMS3000 unit has a backup battery that will support **24 hours** of continued operation. Additionally, to prevent loss of data in the event of disconnection from telecommunication networks, the unit is also equipped with an event memory that can retain up to four (4) days of tests with date and time stamps. These results will be automatically and immediately transmitted to the monitoring system upon restoration of communications, including date and time of occurrence. Additionally, the MEMS3000 operates via standard 110 AC house current. In the event of a power outage, the MEMS3000 unit has a backup battery that will support **24 hours** of continued operation.
4b.0	**SECTION D ALCOHOL MONITORING TRANSDERMAL EQUIPMENT AND SERVICE** **Equipment Requirements - for single body-attached device with or without receiver**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
4b.1	Equipment	Vendor is offering the following Transdermal alcohol monitoring a single body-attached device and as identified in the Price Worksheets. The responses to the following specifications are for this equipment. **Alcohol Monitoring Transdermal Equipment** Single Body-attached Device: Product Bid: Mfg.: _____ Brand/Model: _____	**Sentinel meets this requirement.** **Alcohol Monitoring Transdermal Equipment** Single Body-attached Device: Product Bid: Mfg.: Alcohol Monitoring Solutions, Inc. Brand/Model: SCRAMx Bracelet **Alcohol Monitoring Transdermal Equipment** Receiver: For Product Bid: Mfg.: Alcohol Monitoring Solutions, Inc. Brand/Model: SCRAMx Home Unit (Landline Receiver)

		Alcohol Monitoring Transdermal Equipment Receiver: For Product Bid: Mfg.: _____ Brand/Model: _____	**Alcohol Monitoring Transdermal Equipment** Receiver: For Product Bid: Mfg.: Alcohol Monitoring Solutions, Inc. Brand/Model: SCRAMx Wireless Modem (Cellular Receiver) Please refer to the letters of support from executives at each of these manufacturer's pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units of each in use with Sentinel government customers. **IMPORTANT SENTINEL ADVANTAGE: Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**!
4b.2	Equipment	The device and all additional equipment shall not be available as an open market item if this could compromise the security of the system.	**Sentinel meets this requirement.** Sentinel is pleased to offer SCRAMx® (Secure Continuous Remote Alcohol Monitor), - a comprehensive transdermal ("through the skin") continuous alcohol monitoring system that also incorporates house arrest capabilities. **Sentinel confirms that the SCRAMx unit and all its components are not commercially available to the general public or open market items.** SCRAMx SCRAMx is the most widely-used and the only scientifically-proven and court-validated continuous alcohol monitoring (CAM) device available today. While other vendors new to CAM may claim their transdermal devices are also "proven and court validated," SCRAMx has an unrivaled record of court admissibility and peer-reviewed research when compared to any other CAM system on the market. SCRAMx tests for alcohol every half hour around the clock. The bracelet then transmits data via a wireless radio-frequency (RF) signal to the SCRAMx base station. When data is received from the base station, it is transmitted to and stored in ScramNET, a web-based application, where offender data is collected, analyzed, and maintained in a secure, central location. ScramNET

			will notify the supervising authority of any alcohol readings, tamper alerts, or equipment malfunctions, so that appropriate action can be taken. In addition, SCRAMx has optional radio frequency (RF) (i.e., house arrest) capabilities, allowing it to monitoring presence or absence within the offender's home, without the need for additional equipment.
4b.3	Equipment	The device shall be currently registered and approved by the Federal Communications Commission (FCC).	**Sentinel meets this requirement.** All of the proposed equipment complies with all appropriate FCC regulations. Sentinel has provided the Identifier Numbers below and copies of the certifications are included in the Exhibits section of this proposal: **Part 15** ▪ SCRAMx Bracelet P8M-SM02 ▪ SCRAMx Base Station P8M-SM03 **Part 68** ▪ SCRAMx Base Station US:AMSMM00BSM0
4b.4	Equipment	The strap and circuitry shall enable the device to immediately notify the monitoring center of any tamper attempt or removal from the offenders' ankle.	**Sentinel exceeds this requirement.** The SCRAMx bracelet is equipped with industry-leading, anti-tamper technology that features five sensors to detect and report attempted tampers. These sensors determine whether the bracelet has been cut, removed, obstructed, or submerged. The bracelet's intelligent self-diagnostic capabilities constantly monitor and report its functionality. Any attempts to tamper with the bracelet or its functionality will be immediately detected by the SCRAMx system. **With SCRAMx, the tamper status is sent with every 15-second transmission to the monitoring center, regardless of what that tamper status is.** If the strap is open, it sends the open strap status. If the strap or buckle gets closed, it sends the closed strap status. **The bracelet is simply reporting what the actual status is at all times.** Additionally, during the course of each day, ScramNET will notify the supervising authority of any alcohol readings, tamper alerts, or equipment malfunctions so they can respond quickly to problem offenders.
4b.5	Equipment	The body-attached ankle bracelet unit must offer a rechargeable or field replaceable battery. If rechargeable, device shall function for approximately twenty-four (24) hours on a 2-hour charge. If replaceable batteries, describe	**Sentinel meets this requirement.** The SCRAMx bracelet used a Lithium CR2, field replaceable, disposable battery. The SCRAMx bracelet battery features include: ▪ Battery Type - Lithium CR2 ▪ Battery Life (CAM only) - 90 days

		the in-use live duration of your proposed battery and the basis for replacement of batteries and/or body-attached ankle bracelet unit including details of the number of small parts (screws, clips, rails, etc) that Officers must replace.	▪ Battery Life (CAM plus RF) - 60 days ▪ Battery Charging Capabilities - Disposable/Not rechargeable ▪ Transmitter has a field replaceable faceplate and battery that can be serviced in the field The SCRAMx bracelet will post a low battery message seven (7) days prior to battery failure, allowing sufficient time for the battery to be replaced. The SCRAMx bracelet is comprised of transmitter, battery, faceplate, and exhaust cap, strap, and two screws. Any Installation or battery replacement only requires one tool, a custom wrench. The battery replacement process can be completed in less than five (5) minutes. It is as simple as swapping out the removable faceplate and battery, and re-attaching it to client's ankle using the supplied custom wrench. Then, the Direct Connect device is place over the bracelet to resume actively monitoring the client.
4b.6	Equipment	Describe all maintenance and/or calibration intervals including steps involved and regularity they must be performed (Example: Replace water vessel inside body-attached ankle bracelet unit, once every 90 days.)	**Sentinel meets this requirement.** Sentinel supplies and specifies proactive replacements of SCRAMx bracelets through officer's attritional in-office contact with offenders at an annual interval in order to proactively reduce officer field time associated with replacement. Sentinel will facilitate all SCRAMx equipment maintenance, including recalibration, to ensure proper working order. Sentinel will perform any standard or routine maintenance and calibrations while the SCRAMx devices are in Sentinel's warehouse. Should a device require scheduled maintenance or calibration while assigned to an agency, Sentinel will issue the agency a "Scheduled Maintenance" Return Materials Authorization at the time the device's maintenance or calibration is due (once per year for recalibration). All maintenance and calibration services will be supplied at no charge to the agency.
4b.7	Equipment	Deleted.	
4b.8	Equipment	The device must be shock resistant, water resistant, and must function under normal atmosphere and environmental conditions.	**Sentinel meets this requirement.** The SCRAMx system is water and shock resistant, durable, and hypoallergenic. Additionally, the SCRAMx bracelet function under all normal atmosphere and environmental conditions and does not have any exposed water chambers or external features that could freeze in colder temperatures or stop functioning if it was subject to adverse wearing conditions (as does the TAD device offered by BI, Inc.). **IMPORTANT SENTINEL ADVANTAGE:** SCRAMx is completely water resistant, and all participants are encouraged to shower as frequently and thoroughly as they want. Furthermore, with over seven (7) years of providing CAM systems monitoring over 155,000 offenders, no one has ever circumvented system by taking a bath or submerging SCRAMx.

4b.9	Equipment	The device shall be capable of sending a signal indicating a low battery condition prior to battery depletion.	**Sentinel meets this requirement.** SCRAMx continuously transmits a signal every 15 seconds to the base station to verify its battery condition. The SCRAMx bracelet will post a low battery message seven (7) days prior to battery failure, allowing sufficient time for the battery to be replaced.
4b.10	Equipment	All communications to and from the device shall be encrypted.	**Sentinel meets this requirement.** All communications to and from the SCRAMx transmitter and base station are encrypted. Any SCRAMx transmitter can be matched to any SCRAMx receiver. Each receiver and transmitter is assigned by matching it the central computer, ScramNET. The SCRAMx receiver has dual internal antennas incorporated into the device to ensure continuous communications between the devices.
4b.11	Equipment	The device may be able to provide two-way communications with the participant as a means of rapid officer response to positive alcohol test results and the basis for Officer contact/intervention? If available, describe specifically how your device communicates and how it is tracked in your proposed system.	**Sentinel meets this requirement via optional solutions.** For WSCA user agencies with the need for 2-way communication as part of transdermal alcohol monitoring, Sentinel offers two optional solutions: ▪ Optional companion mobile phone paired with SCRAMx at an incremental additional/optional fee. ▪ Access to the optional CAM Patrol Plus™ Transdermal Alcohol Monitoring system from Sentinel that includes integrated two-way voice communications capability with the participant. During the course of each day, ScramNET will notify the supervising authority of any alcohol readings, tamper alerts, or equipment malfunctions so they can respond quickly to problem offenders. Additionally, all data received from the SCRAMx bracelet through ScramNET is subject to a rigorous data analysis and review process conducted by a team of professionally-trained analysts. These analysts understand the nuances of real-world bracelet use, and can confirm or not confirm drinking episodes using court-proven criteria. T heir review process identifies the presence of environmental alcohol and looks at key characteristics of the Transdermal Alcohol Concentration (TAC) curve– which is similar to a BAC (Blood Alcohol Content) to ensure that only true drinking episodes are confirmed (such as alcohol absorption and elimination rates). All confirmed alcohol violations are automatically date- and time-stamped, sent to agency supervising authorities by 8:00 am the following day via the communications method and medium chosen by the agency. A Daily Action Plan (DAP) typically delivered via email every day, shows which offenders had specific violations.
4b.12	Equipment	The device shall be able to detect and	**Sentinel exceeds this requirement.** The SCRAMx bracelet is equipped with

		record an alert feature with immediate tamper notification including strap tampers, activation and deactivation tampers, and removal tamper notifications. Describe your specific method(s) of tamper detection (Examples: Temperature, Infra-red, etc.) and tamper evident capabilities.	industry-leading, anti-tamper technology that features five sensors to detect and report attempted tampers. These sensors determine whether the bracelet has been cut, removed, obstructed, or submerged. Any attempts to tamper with the bracelet or its functionality will be immediately detected and reported by the SCRAMx system through the following notifications: ▪ Equipment Tamper (bracelet or base station): ▪ Base Station Housing Tamper ▪ Base Station Housing Restored ▪ Open Strap Detected (initial detection) ▪ Bracelet Strap Open (details date and time) ▪ Bracelet Strap Remains Open (after 24 hours) ▪ Bracelet Strap Closed (date and time of replacement With SCRAMx, the tamper status is sent with every 15-second transmission, regardless of what that tamper status is. If the strap is open, it sends the open strap status. If the strap or buckle gets closed, it sends the closed strap status. The bracelet is simply reporting what the actual status is at all times **IMPORTANT SENTINEL ADVANTAGE:** The SCRAMx intelligent self-diagnostic capabilities will report the events regarding the successful installation of the equipment: ▪ Installation Complete ▪ Installation Incomplete ▪ Extending Pending Assignment – Base Station (if base station isn't put into the Assigned to Client status within 24 hours after being put into the Pending assignment status) ▪ Extending Pending Assignment – Bracelet **IMPORTANT SENTINEL ADVANTAGE:** The SCRAMx intelligent self-diagnostic capabilities also constantly monitor and report its functionality and will report the following equipment issues: ▪ Base Station Called from Wrong Number ▪ Missed Check-in Call ▪ Base station Self-Test Failure – Replace
4b.13	Equipment	The device shall be able to detect and record an alert feature with immediate	**Sentinel exceeds this requirement.** SCRAMx continuously transmits a signal every 15 seconds to the base station to verify its battery condition. The

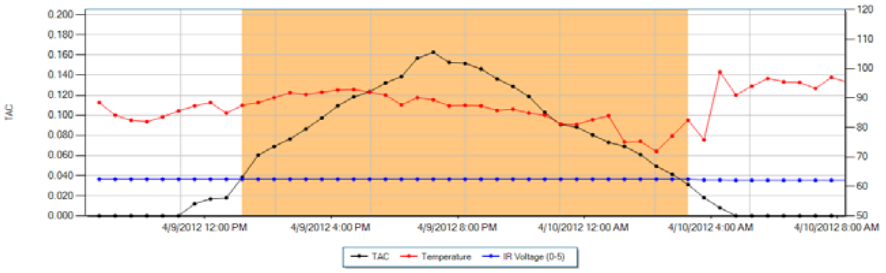
		alert notification for a low battery.	SCRAMx bracelet will post a low battery message seven (7) days prior to battery failure, allowing sufficient time for the battery to be replaced.
			
			IMPORTANT SENTINEL ADVANTAGE: The SCRAMx base unit power supply has been designed specifically to ensure that the power cord will not become disconnected. The SCRAMx receiver contains a backup battery that will function up to 48 hours during a power outage with a fully charged battery, storing messages in its non-volatile memory. When electrical power is restored, the base-station will switch back to main power and a "Power Restore" message will be called into ScramNET and notified per procedures.
			
			The SCRAMx system can be set to notify immediately within 15 minutes on the following alerts/violations regarding the transmitted or base station power and/or battery depletion.
			
			▪ Equipment Loss/Restore (AC Power)
			  ▪ Power Loss
			  ▪ Power Restore
			▪ Voltage Levels
			  ▪ Low Bracelet Battery
			  ▪ Low Base Station Battery

4b.14	Equipment	The device should incorporate non-volatile memory capable of storing at least 24 hours worth of events (with date and time of occurrence) at times when the cellular service or electrical power may become unavailable. In particular, non-volatile memory will retain unreported events and report them once power/cellular services have been restored, including date & time of occurrence.	**Sentinel exceeds this requirement. The SCRAMx bracelet will store up to a month's worth of court admissible alcohol data.** These messages are stored in non-volatile memory and remain there even if the battery goes completely dead. This equates to about 48 tests per day, or 1440 tests per month Additionally, the SCRAMx receiver contains a backup battery that will function up to 48 hours during a power outage with a fully charged battery, storing messages in its non-volatile memory. When electrical power is restored, the base-station will switch back to main power and an "AC Power Restore" message will be called into ScramNET and notified per procedures. All SCRAM events are reported with date and time. **During all power or communication outages, all messages are stored in the receiver's non-volatile memory so that the messages are never lost. The SCRAMx bracelet and receiver will store events and alcohol data for at least one (1) month. All messages are time-stamped.**

			All stored events will be reported to the monitoring center once power/communications have been restored, including the date and time of occurrence.
4b.15	Equipment	All straps utilized to attach equipment to an offender shall be designed so that if an offender cuts, severs or otherwise compromises the integrity of the strap an alert is generated.	**Sentinel meets this requirement.** With SCRAMx, the tamper status is sent to the monitoring center with every 15-second transmission, regardless of what that tamper status is. If the strap is open, it sends the open strap status. If the strap or buckle gets closed, it sends the closed strap status. **The SCRAMx bracelet simply reports what the actual tamper status of the bracelet is at all times.** The SCRAMx strap is made from thermoplastic elastomer comprised of cross linked EPDM rubber and polypropylene. The strap cannot be cut, or attempted to be cut, without leaving physical signs of evidence, as there is no way for such a strap to be put back together again once it has been cut.
4b.16	Equipment	Straps used to attach the equipment to an offender shall have exterior surfaces made of hypoallergenic materials, and shall be adjustable in length to fit all offenders All straps designed to attach equipment to an offender shall have the capability to be securely sized to an offender. If straps are pre-sized they should be immediately available in one-half inch increments or less.	**Sentinel meets this requirement.** SCRAMx straps are made of hypoallergenic material, and are extremely durable and tamper-resistant. The straps are adjustable in four (4) millimeter increments (about 1/6th of an inch) and are simply tightened or loosened to fit any leg.
4b.17	Equipment	System shall measure the ethanol concentration in a discrete sample of the ethanol vapor as insensitive perspiration or the unnoticed perspiration that occurs continuously and shall be obtained via body-attached device without the need for active participation by the participant. The device must be able to distinguish between environmental factors and actual consumption.	**Sentinel exceeds this requirement.** SCRAMx tests for alcohol consumption by measuring the concentration of ingested alcohol present in the insensible perspiration that is constantly produced by the skin. SCRAMx automatically collects these samples of perspiration from the air above the offender's skin and transmits this data to a central source for analysis − requiring no effort on the part of the offender or the supervising agency. Because the human body excretes approximately one percent (1%) of the alcohol they drink through their sweat, if an individual has been drinking it shows up in the level of ethanol vapor present in this insensible perspiration. **Industry-validated Draeger fuel cell**: The Draeger fuel is the heart of the SCRAMx bracelet, which has been proven through decades of research and experience and is accepted by the forensic community in alcohol testing applications. This is the same fuel cell used in evidential breath testing equipment and interlock devices. Draeger fuel cells have been independently

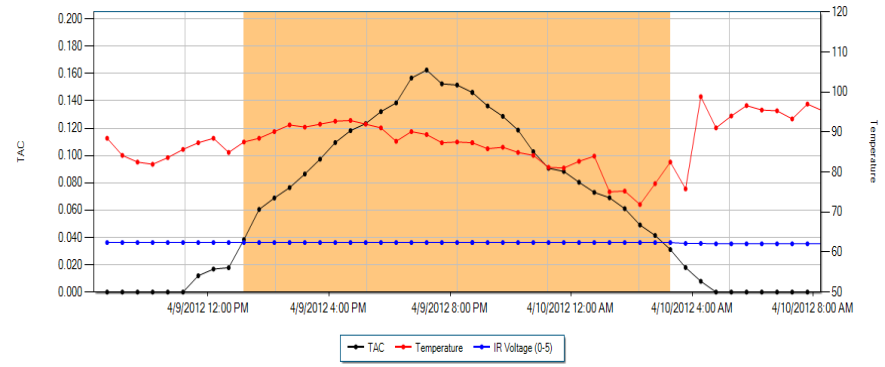
validated (both directly and indirectly), and are extremely sensitive and ethanol-specific alcohol sensors.

Confirmed Alcohol Consumption: Data from a drinking event shows a gradual increase in alcohol levels over time, achieves a maximum TAC and then slowly burns off to create a well-defined alcohol curve. In next graph, TAC is represented by the black line; IR is represented by the blue line, and temperature is represented by the red line.



Confirmed Alcohol Consumption Event: Data from a drinking event shows a gradual increase in alcohol levels over time, and then slowly burns off to create a well-defined alcohol curve (the black

Environmental Alcohol Detection: The following graph depicts an offender coming into contact with an environmental alcohol source (like lotion, mouthwash, etc.). It shows a distinct and dramatic jump in the absorption side of the alcohol curve, followed by a rapid dissipation of the alcohol, unlike the previous graph of an actual drinking event. It shows absorption and burn-off rates outside of the tested, proven rates for consumed alcohol.

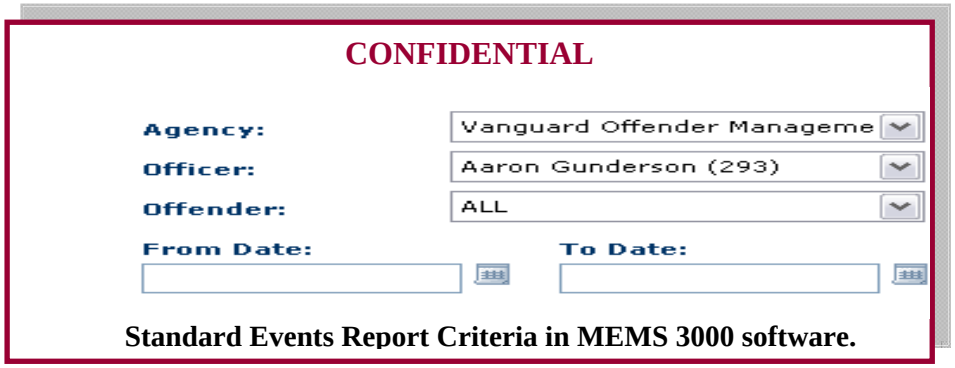
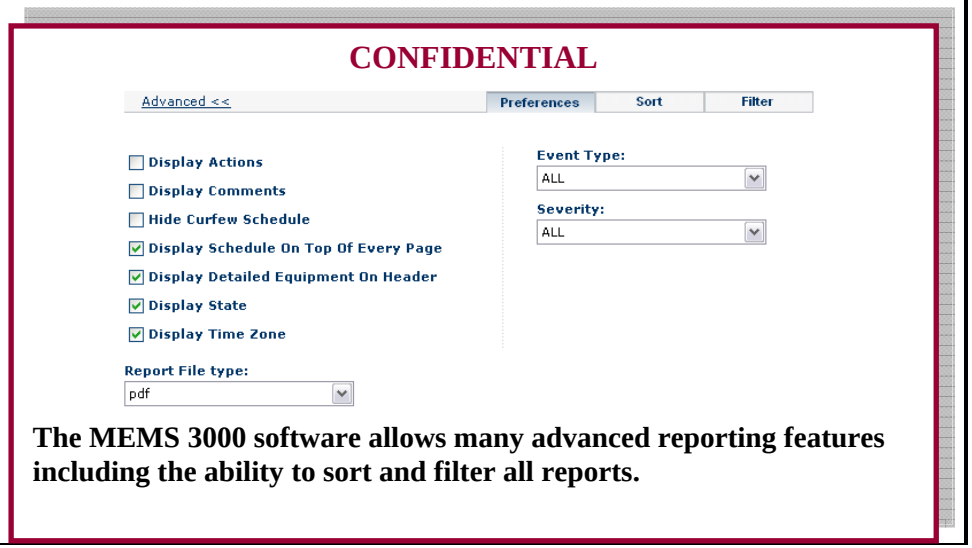
			 **Environmental Alcohol Detection:** This graph depicts an offender coming into contact with an environmental alcohol source. The black line shows a distinct and dramatic jump in the absorption side of the alcohol curve, followed by a rapid dissipation of the alcohol. **Thorough Data Analysis and Review Process:** All data received from the SCRAMx bracelet through ScramNET is subject to a rigorous data analysis and review process conducted by a team of professionally-trained analysts. These analysts understand the nuances of real-world bracelet use, and can confirm or not confirm drinking episodes using court-proven criteria. Their review process identifies the presence of environmental alcohol and looks at key characteristics of the Transdermal Alcohol Concentration (TAC) curve– which is similar to a BAC (Blood Alcohol Content) to ensure that only true drinking episodes are confirmed (such as alcohol absorption and elimination rates).
4b.18	Equipment	The device shall provide for testing to be automatically conducted at fixed intervals that can be set by the Officer on a per participant basis based on the risk of the participant, as frequently as once every 30 minutes. Describe the number of settings, duration of each interval, the steps involved for an Officer to vary the testing intervals, including but not limited to the steps involved, any time delay or conditions for changes in testing interval to become effective, and whether or not	**Sentinel exceeds this requirement.** The SCRAMx device takes an alcohol reading every 30 minutes, 24 hours a day. The process is entirely passive, and requires no action or responsibility on the part of the offender. Because both sensible (liquid) and insensible (gas) perspiration are continuously being collected by SCRAMx during the time between each 30 minute sample, SCRAMx is truly a continuous transdermal alcohol monitoring device. In fact, SCRAMx is the only CAM device on the market that uses a controlled, quantifiable sampling method that draws a measured sample every 30 minutes. In contrast, other vendor's devices may claim to be "testing" more frequently; however, without a controlled, quantifiable sample, **their devices are merely sensors and can present the following issues for agencies:**

		there is a need for monitoring center involvement to vary testing intervals.	▪ These devices are more susceptible to environmental false alerts. ▪ These devices may require secondary tests to validate their results. **IMPORTANT SENTINEL ADVANTAGE:** Competing continuous alcohol monitoring (CAM) systems have vastly different designs than SCRAMx. Most notably is the lack of a "controlled sample". Instead of a quantity of perspiration being tested, similar to a blood, urine, or breath test, they employ a "sensor" (or more specifically, a "proton exchange membrane"). This sensor is always “on” - somewhat like a thermometer. Because such devices lack a quantifiable, controlled sample they have to be “on” in order to constantly check for changes in voltage on the skin. This is often pitched to customers as a benefit when compared to SCRAMx - because where SCRAMx draws and tests the controlled sample every 30 minutes, the competition claims its sensor takes a "reading" every minute. Simple math and clever marketing would lead one to believe that once every minute is better than once every 30 minutes. In actuality, the same reasoning can be applied to SCRAMx, as the collection chamber is gathering insensible perspiration from the wearer each and every second in a controlled sample environment. This controlled volume of perspiration is then drawn and blown across a Draeger fuel cell every 30 minutes and tested for a specific transdermal alcohol concentration (TAC) in the same manner a breath test is given. The sample is then expelled from the device when the collection chamber is empty, and the body continues to refill the chamber with another quantifiable "controlled sample" of insensible perspiration that is constantly being expelled from the body. This is truly continuous alcohol monitoring (CAM). In addition, the SCRAMx fuel cell takes a "pre-test fire" before every test; meaning, that if any environmental alcohol is present, the fuel cell will read it prior to taking the reading from the collection chamber. This, in addition to SCRAMx’s strict absorption and elimination rate criteria, allows a unique advantage in being able to conclusively distinguish between environmental and ingested alcohol. Other competitors’ attempts to provide a transdermal device, who do not have a quantifiable, controlled sample -- and no pre-fire fuel cell located away from the body -- have to rely solely on "algorithms" applied to a sensor resting directly on the skin and exposed to the environment to determine if they believe the change in voltage on the skin is a result of consumed alcohol or environmental.
4b.19	Equipment	The results of each test shall be reported	**Sentinel exceeds this requirement.** Events are reported the monitoring system

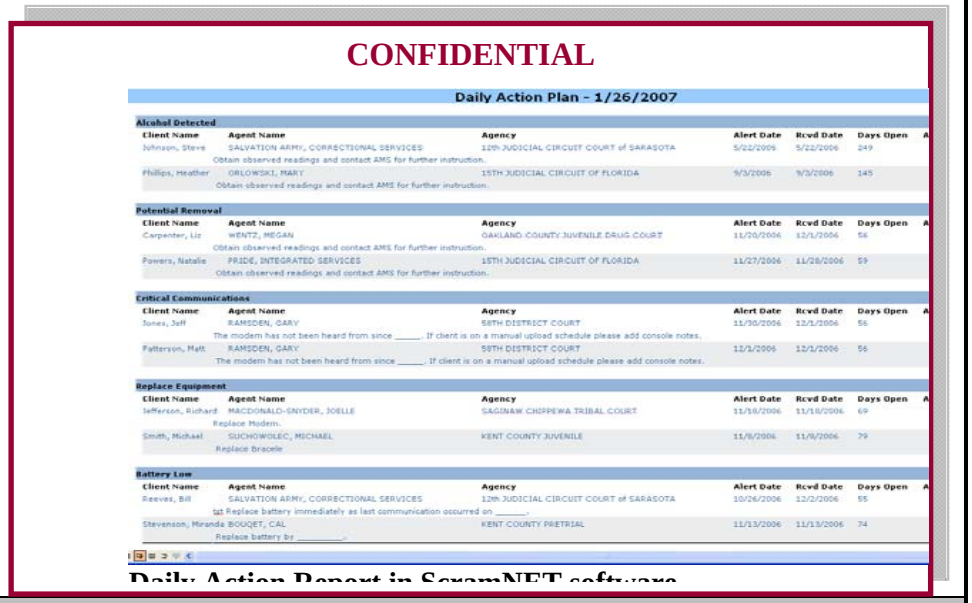
		to the monitoring center and notifiable to Officers. Describe if your device has a cellular reporting connection capable of immediate reporting or, if the test results must be stored in the body-attached ankle bracelet unit and capable of reporting only when the body-attached ankle bracelet returns in range of a second component attached to the participant's home phone landline or cellular line. Describe the number of reporting settings, duration of each reporting interval, the steps involved for an Officer to vary the reporting interval, including but not limited to any time delay or conditions for changes in reporting interval to become effective, and whether or not there is a need for monitoring center involvement to vary the reporting interval.	through the SCRAMx base station (i.e. receiver) which can be easily installed in the participant's residence. The SCRAMx system offers reporting settings of 1 to 6 communication times throughout the day. These client settings establish the times that the bracelet and base station will communicate with each other. Any alcohol events received by the base station are immediately uploaded to ScramNET. The settings can be adjusted by the officer through ScramNET. The default is approximately four hours.
			
			Once detected, all violations including drinking events, tampers, obstructions, communication alerts, and interfering environmental alcohol are reported to the monitoring center and are notifiable to the officers. Additionally, all alcohol-related events are viewed and interpreted by a committee of certified analysts. This ensures that alert notifications are reliably confirmed as valid, so that no additional follow-up testing is needed to confirm drinking events. All confirmed alcohol violations are automatically date- and time-stamped, and typically sent to agency supervising authorities by 8:00 am the following day per agency procedures. A Daily Action Plan (DAP) typically delivered via email every day, shows which offenders had specific violations.
			
			The SCRAMx system can be set to notify immediately within 15 minutes on the following alerts/violations.
			
			▪ Client Movement – this category covers the following alert types:
			  ▪ Unauthorized Leave
			  ▪ Return from Unauthorized Leave
			  ▪ Failed to Leave
			  ▪ Late Leave
			  ▪ Unauthorized Return
			  ▪ Failed to Return
			  ▪ Late Return
			
			▪ Equipment Tamper (bracelet or base station):
			  ▪ Base Station Housing Tamper
			  ▪ Base Station Housing Restored
			  ▪ Open Strap Detected (initial detection)
			  ▪ Bracelet Strap Open (details date and time)
			  ▪ Bracelet Strap Remains Open (after 24 hours)
			  ▪ Bracelet Strap Closed (date and time of replacement)

			▪ Equipment Issue
			  ▪ Base Station Called from Wrong Number
			  ▪ Missed Check-in Call
			  ▪ Base station Self-Test Failure – Replace
			
			▪ Equipment Status
			  ▪ Installation Complete
			  ▪ Installation Incomplete
			  ▪ Extending Pending Assignment – Base Station (if base station isn't put into the Assigned to Client status within 24 hours after being put into the Pending assignment status)
			  ▪ Extending Pending Assignment – Bracelet
			
			▪ Equipment Loss/Restore
			  ▪ Power Loss
			  ▪ Power Restore
			  ▪ Telephone Restore (as general interruption of telephone service is not uncommon)
			
			▪ Voltage Levels
			  ▪ Low Bracelet Battery
			  ▪ Low Base Station Battery
			
			IMPORTANT SENTINEL ADVANTAGE: SCRAMx is the latest continuous transdermal alcohol monitoring device with cellular communication capabilities, as well as via landline. Sentinel will offer SCRAMx Wireless which communicates via cellular network to monitor all offenders placed on the program. The wireless device simply plugs into an electrical outlet, and the data will download daily at the scheduled time and upload directly to ScramNET.
			
			IMPORTANT SENTINEL ADVANTAGE: The SCRAMx unit is the only transdermal unit that can function without a residential telephone line or cellular service. Through its Direct Connect computer access, results can be downloaded via laptop or desktop computer by authorized personnel at any location, at anytime. Other transdermal devices are tied to home base stations that require telephone service.
			
			SCRAMx Direct Connect: In cases where an offender does not have access to

			a landline or poor cellular reception, he or she can come into the supervising authority's office to have data that has been stored in the bracelet downloaded via the SCRAMx Direct Connect device. The compact Direct Connect device is slipped over the offender's bracelet (while worn) and attached by USB cable to an internet-enabled computer. The stored information is then transmitted from the SCRAMx bracelet directly for review without the need for a base station.
5.0	**SECTION E System Reports**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
5.1	Equipment Inventory Reports	A system that allows the Agency to generate the following "canned" reports directly from the Vendor's database through the secure internet site. To ensure that reports are accurate and timely, the system's database shall be updated in real time to ensure all report data is current when viewed and/or downloaded by the Agency's personnel. All reports shall have the capability of being queried, sorted or filtered by any field contained in the report or by data parameters as applicable and reports shall be readable on screen, printable and shall be downloadable into an excel format.	**Sentinel exceeds this specification.** Authorized users have the ability to directly access all participant historical information through Sentinel's remote alcohol computer software system database or ScramNET. All monitoring standard reports are available through the proposed software's easy-to-use report generator applications in a standard transaction file format. Participant monitoring information can be queried and filtered to meet the report needs of each participating agency. Sentinel will work with its clients to ensure all needed reports, including on-demand, daily and quarterly reports are available. Any authorized user can view participant activity 24 hours a day, seven (7) days a week, 365 days a year. Participant activity is posted **in real-time**, so that agencies always have the latest information and users can view violations online as they occur. In addition to "canned" reports, SCRAMNET provides a wide range of "instant" reports and graphs – from a snapshot of a single event to a comprehensive view of an offender's behavior over time. All ScramNET reports can be viewed online, printed, saved, and emailed /or downloaded as PDFs, Excel files or Word documents.
5.2	Equipment Inventory Reports	The system must be able to provide real time reports of all assigned equipment. Report shall include description/type of equipment, serial number, assigned Offender, and assigned Officer.	**Sentinel exceeds this specification.** Authorized users have the ability to directly access all assigned equipment information including the description/type of equipment, serial number, assigned offender, and assigned Officer through Sentinel's remote alcohol computer software system database or ScramNET. Any authorized user can view these reports 24 hours a day, seven (7) days a week, 365 days a year. Inventory is posted **in real-time**, so that agencies always have the latest information. Sentinel confirms that the MEMS 3000 software provides an Equipment report and ScramNet provides a Current Inventory Report that sorts the entire inventory by servicing location and status at the time the report is run.

			Additionally, ScramNET provides several reports to assist agencies with inventory reconcilitation. The Inventory Tracking Report assists as a checklist while conducting a physical inventory and verifying the status of all equipment. It can be sorted by device type and/or inventory status.
5.3	Notification Report	The Vendor's system shall provide the Agency the ability to generate a report by date parameters, sorted by location site, identifying the number and type of notifications during specified time parameters, such as: • Monday-Friday, 8:00 am-5:00 pm • After hours • Weekends And indicating summary totals for: • Total number of alerts per location site, percent of total per type of alert and average number of alert notifications per month, per offender within each location site.	**Sentinel meets this requirement.** Sentinel confirms that the MEMS3000 software will allow all authorized users to generate an events report with the ability to sort by agency (location), officer (or all officers), offenders (or all offenders) within specified date ranges.  **Standard Events Report Criteria in MEMS 3000 software.** If more information is necessary then select the "Advanced" button and more fields will be appear with added criteria  **The MEMS 3000 software allows many advanced reporting features including the ability to sort and filter all reports.**

			ScramNET also offers several reports to assist agencies with notification information. The Agency Activity Report displays the number of alerts generated by all of clients (by date) assigned to an agent/officer. The Activity by Agency Report supplies different alert summary numbers for positive, tamper, and equipment alerts for a client during a specified date range. Currently, there is no report that gives an average number of alert notifications in ScramNet; however, Sentinel will work with the agency to provide this report as necessary.
5.4	Offender Alert Report	The Vendor's system shall provide the Agency the ability to generate alert reports, queried by individual assigned offender and date parameters that identifies the type of alert, time of alert, method of alert (fax, e-mail or phone call) and recipient of alert.	**Sentinel meets this requirement.** The MEMS3000 software will allow all authorized users to generate an events report with the ability to sort by agency (location), officer (or all officers), offenders (or all offenders) within specified date ranges. Through the Advanced" criteria screen, users can choose to view all actions taken based on the event (i.e. faxed or email alert to a particular recipient) and/or comments associated with alert resolution. **IMPORTANT SENTINEL ADVANTAGE:** Should an officer or supervisor only be interested in open violations (not resolved), the MEMS3000 software allows authorized users to create an on-demand "Open Violations" report. Additionally, Sentinel confirms that the Client Report displays all alerts for a specific client for a defined period of time. The Non-Compliance Report provides very detailed information for a specific client alert.
5.5	Customized Reports	The Agency can request custom reports the cost of which (if any) shall be established between the Vendor and the Agency Program Manager.	**Sentinel meets this requirement.** Sentinel will provide customized optional on-demand reports with user defined fields as requested by the participating agency at minimal cost (if any).to assist with the monitoring of participants and/or the monitoring of program effectiveness.
5.6	Offender Report	The Vendor's system shall provide the Agency the ability to generate a summary report of all offenders and/or assigned officer that identifies offender name, Agency number, address, and officer assigned.	**Sentinel meets this requirement.** Sentinel confirms that the MEMS3000 software includes an on-demand summary "Offender List" report that identifies offender name, Agency identifier, address, and officer assigned. Additionally, Sentinel confirms that the "Client Summary for Agency Report" in ScramNet provides this information.
5.7	Current Usage Report	The Vendor's system shall be able to provide the Agency the ability to generate a current usage report indicating the actual number of daily service units used to date (real time) for the monthly period. This report should be detailed to reflect offender name, Agency number, service	**Sentinel meets this requirement.** Sentinel confirms that the MEMS3000 software includes an on-demand summary "Offender Program" report. Sentinel will provide each participating agency with a current usage report indicating the actual number of daily service units used to date (real time) for the monthly period reflecting offender name, Agency identifier, service type (active) and number of days utilized to date. Additionally, Sentinel confirms the "Client Summary for Agency Report" in ScramNet also provides this information.

		type (active) and number of days utilized to date.	
5.8	Daily Alert Summary Report	The Vendor shall submit a daily report (between the hours of midnight and 6:00 a.m. for the previous day) that identifies each alert, type of alert, time and duration of alert, assigned officer, assigned offender, and totals. This report shall be sorted by location sites region/unit/officer and shall be e-mailed to all designated officers within the location sites.	**Sentinel meets this requirement.** Sentinel will submit a daily report for both remote and transdermal alcohol monitoring (between the hours of midnight and 6:00 a.m. for the previous day) that identifies each alert, type of alert, time and duration of alert, assigned officer, assigned offender, and totals to each participating agency as is applicable based on agency utilization and notification/reporting requirements. This report shall be sorted by location sites region/unit/officer and shall be e-mailed to all designated officers within the location sites. Please see the following example "Daily Action Plan" that provides this information.  CONFIDENTIAL Daily Action Plan - 1/26/2007 Alcohol Detected Client Name / Agent Name / Agency / Alert Date / Rcvd Date / Days Open Johnson, Steve / SALVATION ARMY, CORRECTIONAL SERVICES / 12th JUDICIAL CIRCUIT COURT of SARASOTA / 5/22/2006 / 5/22/2006 / 249 Obtain observed readings and contact AMS for further instruction. Phillips, Heather / ORLOWSKI, MARY / 15TH JUDICIAL CIRCUIT OF FLORIDA / 9/3/2006 / 9/3/2006 / 145 Obtain observed readings and contact AMS for further instruction. Potential Removal Client Name / Agent Name / Agency / Alert Date / Rcvd Date / Days Open Carpenter, Liz / WENTZ, MEGAN / OAKLAND COUNTY JUVENILE DRUG COURT / 11/20/2006 / 12/1/2006 / 56 Obtain observed readings and contact AMS for further instruction. Powers, Natalie / PRIDE, INTEGRATED SERVICES / 15TH JUDICIAL CIRCUIT OF FLORIDA / 11/27/2006 / 11/28/2006 / 59 Obtain observed readings and contact AMS for further instruction. Critical Communications Client Name / Agent Name / Agency / Alert Date / Rcvd Date / Days Open Jones, Jeff / RAMSDEN, GARY / 58TH DISTRICT COURT / 11/30/2006 / 12/1/2006 / 56 The modem has not been heard from since _____. If client is on a manual upload schedule please add console notes. Patterson, Matt / RAMSDEN, GARY / 58TH DISTRICT COURT / 12/1/2006 / 12/1/2006 / 56 The modem has not been heard from since _____. If client is on a manual upload schedule please add console notes. Replace Equipment Client Name / Agent Name / Agency / Alert Date / Rcvd Date / Days Open Jefferson, Richard / MACDONALD-SNYDER, JOELLE / SAGINAW CHIPPEWA TRIBAL COURT / 11/18/2006 / 11/18/2006 / 69 Replace Modem. Smith, Michael / SUCHOWOLEC, MICHAEL / KENT COUNTY JUVENILE / 11/8/2006 / 11/8/2006 / 79 Replace Bracele Battery Low Client Name / Agent Name / Agency / Alert Date / Rcvd Date / Days Open Reeves, Bill / SALVATION ARMY, CORRECTIONAL SERVICES / 12th JUDICIAL CIRCUIT COURT of SARASOTA / 10/26/2006 / 12/2/2006 / 55 1st Replace battery immediately as last communication occurred on _____. Stevenson, Miranda / BOUQET, CAL / KENT COUNTY PRETRIAL / 11/13/2006 / 11/13/2006 / 74 Replace battery by _____. Daily Action Report in ScramNET software
6.0	**SECTION F Equipment Testing, Replacements, Lost/Damaged/Stolen Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
6.1	Equipment Accessories	The Vendor shall provide all necessary supplies and replacement supplies and instruction/training materials at no additional costs to the Agency.	**Sentinel meets this requirement.** Sentinel will provide all necessary alcohol monitoring equipment supplies, replacement supplies and instruction/training materials when necessary or upon request depending on the item at no additional costs to the participating agency.
6.2	Equipment Spare Inventory	The Vendor shall provide and maintain a backup/replacement inventory of	**Sentinel meets this requirement.** Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-

		monitoring units equal to fifteen percent (15%) of the actual number of units currently in use in each the Agency's Location sites/Office locations at no additional cost. The Agency shall not pay the Vendor an inventory fee, storage fee, installation equipment fee or any other fee related to these inventory units and equipment.	site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. Sentinel understands that no agency will be required to pay an inventory fee, storage fee, installation equipment fee or another fee related to inventory units/spare equipment. Sentinel acknowledges that participating agencies shall only pay the per-day unit rate on activated units as set forth in the contract.
6.3	Replacement Equipment	The Vendor shall assure that all equipment delivered to the Agency has been tested to ensure it is operable, free from any defects or damage and is fully operational. The Agency reserves the right to reject any and all equipment not determined to be operational and in acceptable operative order and condition. In the event any equipment becomes inoperative due to a malfunction or through normal use, the Vendor shall incur all replacement costs and repairs. The Vendor shall provide the Agency with replacement equipment within 24 hours at no charge to the Agency, including shipping and handling costs for both delivery and return.	**Sentinel meets this requirement.** Sentinel confirms that all equipment provided to WSCA participating agencies will be covered by a full manufacturer's warranty **for the length of any contract**. Sentinel will maintain all equipment in good operating condition, free from materials defects and/or workmanship under normal use and fully operational for the term of this agreement. Sentinel understands that the participating agencies reserve the right to reject any and all equipment not determined to be operational and in acceptable operative order and condition. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. Sentinel's assigned Account Manager will work proactively with each Western States Contracting Alliance participating agency to ensure the appropriate amount of equipment and spares are maintained for the electronic monitoring of offenders. This open communication aids Sentinel in assuring ample equipment is available to meet each agency's needs. In the event of any malfunction of any piece of equipment, Sentinel will provide routine equipment maintenance repair through the return and replacement of malfunctioning equipment at no additional cost to participating agencies. Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite**

			replacements of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. **Additionally, if any agency's spare inventory is depleted, Sentinel will re-supply the appropriate equipment via overnight delivery at no additional cost within 24 hours after notification.** All shipping costs (both delivery and return) of all equipment and supplies will be the responsibility of Sentinel. **Product Warranty:** Sentinel represents and warrants that, upon delivery of any product and/or consumable to the delivery location, such product will have been manufactured, filled, packaged, stored and shipped materially in accordance with the specifications or custom specifications for such product in accordance with the associated purchase order. Sentinel further represents and warrants that it shall obtain and maintain all necessary licenses, permits or approvals in connection with the manufacture, filling, packing, testing, storage and shipment of each such product. **Sentinel warrants all of its equipment and software for the life of the contract.** This includes software maintenance, licensing and future feature enhancements. **Warranty Service:** Warranty service with Sentinel is a very simple process. The participating agency only needs to contact the proposed Account Manager to discuss warranty service and/or feature upgrades. Sentinel is committed to the continual development of feature enhancement and product development. The Account Manager will also work with the Sentinel training department to provide any training required by a new feature or upgrade to the equipment or system.
6.4	Lost/Damaged/Stolen	At no additional cost, the Vendor shall supply replacements for lost, stolen and damaged equipment up to five percent (5%) per year of the Agency's active units. The Vendor shall have three (3) working days to replenish requested stock. All units shall be maintained at the Agency's office for use as immediate	**Sentinel meets this requirement.** Sentinel will provide an annual 5% allowance of the daily average of active units per year to each Western States Contracting Alliance participating agency for lost, damaged and/or stolen equipment replacements. Sentinel requests the opportunity to work closely with each participating agency to ensure programmatic and participant policies achieve this level. Based upon Sentinel's experience in other contracts, Sentinel has found a few points essential to improved management of equipment inventory and loss, damaged or stolen equipment. This includes

		replacements, when needed. Vendor must detail within their Price Sheet the per component replacement cost for each component of every proposed equipment model. This replacement cost shall be applied for any excess losses above the allowed annual 5% lost, stolen and/or damaged equipment replacements.	increased emphasis to not remove the transmitter until all pieces of equipment provided to the participant are together in the same place, either at the participant's home or the participating agency office location. Sentinel would request ongoing coordination with participating agency for participants to return equipment to the participating agency office. Additionally, Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment and will be replenished within three (3) working days should the stock become depleted. Sentinel has provided the per-component cost for lost, stolen or damaged replacement equipment in excess of the annualized 5% allowance in the pricing section of this proposal should payment be required.
7.0	**SECTION G Training Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
7.1	Training	Vendor shall provide initial on-site training by experienced staff with thirty (30) days of start of Agency's contract, unless an alternate training schedule is agreed upon. Additional on-site training via webinar shall be provided within 48 hours of request. Ongoing training shall be provided as agreed mutually between vendor and agency.	**Sentinel meets this requirement.** Sentinel is committed to working in partnership with each participating agency utilizing the Western States Contracting Alliance contract over the term of the contract to make sure that all staff are fully and properly trained on the operation and installation of the proposed equipment, the use of the software for participant management, and interpretation of violation notifications and reports along with all other needed training requirements. Sentinel will provide initial on-site training has included a sample written training curriculum in the Exhibits section of this proposal for the Western States Contracting Alliance to review and consider. Initial on-site training will be enacted prior to the implementation of the services. In Sentinel's experience, initial training should be conducted in near-proximity to intended program start date and be conducted to ensure that all agency personnel are completely comfortable and knowledgeable in using the proposed equipment and systems therefore Sentinel will provide initial training within 30 days of the Notice to Proceed commencement date, unless an alternate training schedule is agreed upon. Initial training includes instruction on the operation of any monitoring equipment and software discussed in this proposal and selected

			for use and implementation by the respective participating agency. Once Sentinel management and participating agency management agree upon program guidelines, notifications, and parameters, Sentinel will arrange for a mutually beneficial training session. Additionally, Sentinel will provide post-deployment on-going training per the established contract at no cost to the participating agency. Any future training will be scheduled in a manner that is beneficial and cost-effective to both the agency and Sentinel. **IMPORTANT SENTINEL ADVANTAGE:** The Sentinel training department offers webinar training sessions for customers and staff on an on-going basis. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
7.2	On-Site Initial Training	Deleted.	
7.3	Onsite Ongoing Training	Deleted.	
7.4	Manuals/ Installation Guides	The Vendor shall provide training and/or user manuals upon each Officer's initial orientation training in hardcopy or soft file format such as PDF may be provided at the request of the Agency. All training and all associated training manuals shall be provided at no cost to the Agency.	**Sentinel meets this requirement.** Sentinel will supply all operational/procedural manuals and training materials, including written instructions and equipment for initial training, to be used by participating agency personnel at no additional cost. Sentinel will also provide all training and/or user manuals in hardcopy or soft format (such as PDF) and provide written authorization to the participating agency to duplicate these materials as necessary to facilitate future agency training needs. In addition for the transdermal alcohol monitoring solution, equipment documentation, troubleshooting materials, and training materials are all available online for immediate 24-hour access. Also a very detailed "Help" page functionality is available through SRAMNet. The content within the Help page is readily maintained. Help features and functionality include: ▪ SCRAMx Operations Guide – Facilitates management of an efficient

			SCRAMx program. ▪ Daily Tasks Guide – Designed for those responsible for managing the day-to-day tasks for clients who are ordered to wear the SCRAMx bracelet. The content is logically grouped by daily, weekly, and quarterly tasks. The guide is not intended to be a comprehensive manual, but rather a concise list of the daily tasks for efficient management of the County's SCRAMx program. ▪ Quick Sheets – Stand-alone procedures that provide step-by-step directions to assist with SCRAMx equipment tasks, such as equipment setup, equipment replacements, and manual data uploads.
7.5	Training Materials	The Vendor shall provide all materials and equipment necessary to perform the training and shall utilize actual equipment currently being utilized. All training manuals may be hardcopies or soft file format, user friendly, and kept up to date with the most current training protocols. Training manuals shall be provided for each Agency staff member trained and upon the request of the Agency Program Manager. The training curriculum and evaluation forms that will be utilized for all training purposed should be submitted by Vendor.	**Sentinel meets this requirement.** Sentinel will supply all operational/procedural manuals and training materials, including written instructions and equipment (actual equipment currently being utilized) for initial training, to be used by participating agency personnel at no additional cost. Sentinel will also provide all training and/or user manuals in hardcopy for each agency staff member trained upon the request of the agency Program Manager or in soft format (such as PDF) and provide written authorization to the participating agency to duplicate these materials as necessary to facilitate future agency training needs. Sentinel confirms all training manuals are user friendly, and kept up to date with the most current training protocols. The training objectives are to provide general knowledge of the technology, scientific principles of the technology, software navigation, and all functional aspects of the hardware/equipment tasks. Topics covered in training include but are not limited to: ▪ Equipment overview ▪ Components of the system ▪ Accessing web-based platforms ▪ Troubleshooting ▪ Region setup (optional) ▪ Agency setup ▪ Agent and agent supervisor setup ▪ Court setup, if needed ▪ Inventory management ▪ Client enrollment ▪ Equipment assignment and installation ▪ Alert management ▪ Equipment maintenance ▪ Data interpretation ▪ Reporting ▪ Judge setup, if needed

			Sentinel has included a sample written training curriculum and evaluation forms in the Exhibits section of this proposal for the Western States Contracting Alliance to review and consider.
7.6	Webinar and Online Training	The Vendor shall make available to officers remote webinar and online training sessions which demonstrate device applications after initial orientation per officer. The Vendor shall provide Webinar online and online. Training for system, software and hardware updates.	**Sentinel meets this requirement.** The Sentinel training department offers webinar training sessions for customers and staff on an on-going basis address attrition and additional training needs as well as for any system, software and hardware updates. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
8.0	**SECTION H Additional Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
8.1	Vendor Staff	The Vendor shall provide an adequate level of staffing for provision of the services outlined herein and shall ensure that staff providing services are highly trained and qualified.	**Sentinel exceeds this requirement.** Sentinel **operates** both its primary monitoring center located in Irvine, California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** **IMPORTANT SENTINEL ADVANATGE:** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a**

			monitoring center failure or service catastrophe. Sentinel is highly experienced in the effective management of this program through its current incumbent radio frequency electronic monitoring program, which provides **a better understanding of the participating agencies' overall monitoring needs than any other vendor in the industry**. Sentinel believes that an expanded partnership with the Western States Contracting Alliance for the **lease of alcohol and GPS monitoring options** not currently available to the department will develop this into a world-class program similar to other programs in the nation and regionally provided through Sentinel. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's monitoring center is staffed with bilingual personnel on every shift in order to ensure successful interactions with its agency customers. Sentinel monitoring center personnel typically answer 96% of all calls within eight (8) seconds and provide an on-hold wait time of four (4) seconds or less. All of Sentinel's monitoring center employees undergo a thorough and detailed training and certification program, during which they are trained in all aspects of electronic monitoring equipment and software including troubleshooting and the necessary alarm procedures to ensure timely and accurate notifications. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel monitoring center staff is cross-trained to support assistance requests for radio frequency (RF) electronic monitoring, voice verification monitoring programs, **breath alcohol testing (BAT), transdermal alcohol monitoring** and global positioning satellite (GPS) tracking should any participating agency be utilizing more than one (1) service category. Two (2) full weeks are used during the training of a new monitoring center operator to ensure that a thorough electronic monitoring knowledge based is developed. Complete equipment functionality and software platform protocols must be understood prior to graduation to a Level One Monitoring Center Operator. The training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge- and performance-based, allowing maximum participation by monitoring center staff and supervisors. The

training techniques, tools, and exams are developed by the training coordinator and are required to successfully complete the certification process. The coordinator will conduct training sessions at regularly scheduled intervals; however, each shift supervisor will be instrumental in the development of their employees.

Monitoring Center On-going Training: To maintain an efficient service oriented organization, Sentinel employs on-going training modules for all positions. This method is applied equally to all monitoring center operators as to allow correct interpretation and dissemination of information to all authorized agency personnel. The training modules for each employee within the monitoring center are delineated. Sentinel is committed to providing the highest level of monitoring services in the industry. A critical element of providing reliable and efficient monitoring is a knowledgeable, professional and well-trained staff.

This training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge and performance based, allowing maximum participation by monitoring center staff and supervisors. A grading system has been established to easily identify staff members with certain knowledge and ability. This grading system requires an employee to demonstrate acquired skills through verbal and written examinations.

Levels:

- Monitoring Specialist Level – Trainee
- Monitoring Specialist Level – 1
- Monitoring Specialist Level – 2
- Monitoring Specialist Level – 3
- Monitoring Shift Supervisor

Training / Certification: The Training Coordinator is responsible for developing the training techniques, tools, and exams that are required to successfully complete the certification process. The Training Coordinator will conduct training sessions at regularly scheduled intervals; however each shift supervisor will be instrumental in the development of their employees. Training for the various levels will be conducted as follows:

Level	Training	Certified By

	Conducted By	
Trainee	Training Coordinator	Training Coordinator
1	Shift Supervisor	Training Coordinator
2	Shift Supervisor	Training Coordinator
3	Training Coordinator	Training Coordinator
Shift Supervisor	Monitoring Center Manager	Monitoring Center Manager

Certification Exams: A written examination is prepared for each grade level. Some grade levels require that an employee demonstrate acquired skills. A minimum test score is required to pass the written examination.

Level	Minimum Score
Trainee	85%
1	85%
2	85%
3 / Shift Supervisor	90%

A passing score is mandatory for the Trainee and Level 1 position and is required for continued employment. The Level 1 certification exam must be successfully completed before the expiration of a new employee's orientation period. Re-testing periods are established to give an employee an additional attempt to achieve a passing score.

Level	Testing Period	Re-Testing Period	Passing Score
Trainee	When initial training complete	14 Days	Mandatory
1	10 weeks' employment	14 Days	Mandatory
2	90 Days	30 Days	Not Mandatory
3	90 Days	30 Days	Not Mandatory

A passing score is mandatory for continued employment beyond the orientation period for the Trainee and Level 1 grade.

Promotion: This performance-based program ensures that qualified candidates are promoted in a manner consistent with Sentinel's goal of maintaining a knowledgeable and professional staff. A staff member will be promoted upon successful completion of the certification process. An employee that meets the length of service requirements for a grade promotion must be recommended for advancement by their supervisor. Supervisors are advised to consider the following items before recommending an employee for promotion.

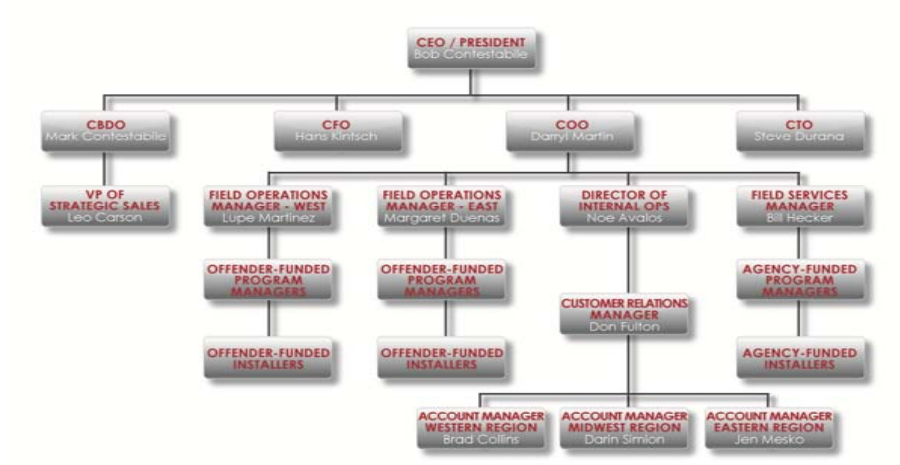
Performance:

- Attendance
- Dependability

Measuring Tools:

- Report
- Charts

Additionally, Sentinel's strong nation-wide presence of qualified field services staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract. The following is a Key Personnel Organizational Chart followed by descriptions of the associated project tasks of Operational Staff responsible for this contract.



Sentinel has a proven track record of providing excellent performance and

			flexibility to its customers and will commit this same dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all services including but not limited to technical assistance, customer support, inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value. **IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness.
8.2	On-Site Service	The Vendor shall provide remote diagnostic support and trouble-shooting technical assistance via a toll-free telephone line 24 hours a day, seven (7) days a week, including holidays. In the event of technical problems that are not resolved from a remote location, the Agency Program Manager, upon request, may require the Vendor to provide on-site, technical assistance within 24 hours.	**Sentinel exceeds this requirement. Staffed customer service and remote diagnostic support through technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** **Additionally, each participating agency will be assigned a liaison field services staff member that will be dispatched to provide on-site service in the event of the need for technical assistance, electronic diagnosis or replacement of component problems within 72 hours of requested service.** **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are staffed and fully operational 24 hours a day.** Sentinel strives to resolve any customer inquiries promptly and on the first contact and the majority of technical problems are resolved through technical telephone support, through remote diagnostics, or through equipment replacement using the on-site spares. Each monitoring center operator has the

			expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, changing a participant's schedule, performing participant enrollments or entering data into the system. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Account Management/Field Services personnel for customer enhancement requests, suggestions and ideas.
8.3	Litigation-Related Testimony	The Vendor shall make available qualified personnel to provide testimony as requested or subpoenaed. Affidavit, expert witness testimony, violation hearing testimony, or any other expert testimony/certification shall be provided at no additional cost to the Agency. The Vendor shall immediately notify the Agency Program manager or designee upon receipt of any subpoena involving or affecting the Agency.	**Sentinel meets this requirement.** Sentinel understands the required testimony obligations, and Sentinel is fully prepared to provide qualified personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports while under oath in a court of law. Should the need occur for testimony in court upon request of the participating agency and/or in response to a subpoena, Sentinel will provide expert court testimony, either in person or written witnesses qualified to defend the integrity of Sentinel systems and services. Sentinel, with 20 years proven experience, has maintained integrity and credibility with numerous courts throughout the country on behalf of the agencies it serves. Sentinel will be able to submit the monitoring documentation as supporting evidence when describing the program participant's activities while alcohol monitoring. Sentinel will immediately notify the participating agency Program Manager or designee upon receipt of

			any subpoena involving or affecting the agency. Additionally, Sentinel request advance written notice from the agency of the need for such testimony if possible. **IMPORTANT SENTINEL ADVANTAGE:** The manufacturers of SCRAMx, Alcohol Monitoring Systems, Inc. (AMS), firmly support SCRAMx monitoring results in court, and are available to offer expert testimony on the science of continuous transdermal alcohol monitoring technology at no additional charge to the county. This means that sanctions can be verified and enforced based on the data received from the SCRAMx device, ensuring single-source admissibility and eliminating the need for a "secondary screen" or additional confirmation of a drinking event. The competition cannot match this track record within the courts. SCRAMx has been upheld in every state in which it has been challenged. To date, SCRAMx – and its predecessor SCRAM − have been found admissible and reliable in: ▪ 89 hearings in 24 states ▪ 33 hearings that resulted in Daubert, Frye, or hybrid rulings ▪ 3 State Supreme and Appellate Court rulings Since 2003, Alcohol Monitoring Systems, Inc. have been working with courts and ancillary agencies to provide comprehensive SCRAMx testimony, which has included the creation of nearly 2,000 formal court reports used to detail the monitoring results of offenders who denied a SCRAMx violation (either alcohol consumption, equipment tampering, or a combination). In the majority of the cases, offenders confronted by the court armed with a comprehensive SCRAMx reporting package admitted to the violation prior to the scheduled hearing. **The following are the latest six (6) hearings where testimony met the Frye Standard for Admissibility:** ▪ Illinois: First Judicial Circuit Court in July 2007 ▪ Florida: Collier County Court in November 2006 ▪ Florida: 20th Judicial Circuit Court in August 2006 ▪ Pennsylvania: Lycoming DUI Court in May 2006 ▪ Georgia: Cherokee County State Court in September 2005 ▪ Florida: Circuit Court of Okaloosa County in September 2005

			The following are the latest 26 hearings where testimony met the Daubert Standard for Admissibility: ▪ Michigan: Berrien County Circuit Court in October 2010 ▪ Oklahoma: Jackson County District Court in July 2010 ▪ Wyoming: Albany County Drug Court in January 2010 ▪ South Dakota: South Dakota Board of Pardons & Parole in November 2009 ▪ South Dakota: Circuit Court of the Sixth Judicial Circuit in November 2009 ▪ Colorado: Greeley Combined Court Division #4 in November 2009 ▪ New Hampshire: Southern Carroll County Superior Court in May 2009 ▪ South Dakota: Circuit Court of the Sixth Judicial Circuit in May 2009 ▪ New York: Clinton County Supreme Court in March 2009 ▪ New York: Clinton County Supreme Court in March 2009 ▪ Ohio: Putnam County Court in January 2009 ▪ Ohio: Putnam County Court in January 2009 ▪ Indiana: Hamilton County Superior Court #5 in December 2008 ▪ Tennessee: Rutherford County Circuit Court in November 2008 ▪ Texas: 114th District Court in July 2008 ▪ Colorado: Westminster Municipal Court in December 2007 ▪ South Dakota: Circuit Court of the Sixth Judicial Circuit in October 2007 ▪ Texas: 238th District Court in July 2007 ▪ Tennessee: Criminal Court 18th Judicial District in June 2007 ▪ Tennessee: General Session 18th Judicial District in March 2007 ▪ Ohio: Common Pleas Court in February 2007 ▪ Oklahoma: Payne County District Court in October 2006 ▪ Ohio: Cleveland Municipal Court in October 2006 ▪ Louisiana: 16th Judicial District Court in September 2006 ▪ Ohio: Fairfield County Common Pleas Court in September 2005 **The following is the latest hearings where testimony met the Hybrid Standard of Frye, Daubert and Frye 702 Admissibility:** ▪ California: Superior Court of San Fernando County in October 2007 With 89 evidentiary hearings in 24 states, 33 hearings resulting in Frye/Daubert

			rulings, as well as one (1) Supreme Court ruling and one (1) Appellate Court ruling, SCRAMx has been upheld in every state in which it has been challenged. This makes it the most court-validated system on the market today. The competition cannot match AMS' track record within the judicial system with any other transdermal alcohol monitoring device.
8.4	Quality Assurance Program	The Vendor shall have a formal quality assurance/quality control program in place that demonstrates that routine evaluations of the quality of the system, equipment and service are performed to ensure compliance with the terms and conditions of the Contract.	**Sentinel exceeds this requirement.** Sentinel has implemented a fully established internal quality assurance/quality control plan addressing all core business operations to demonstrate its willingness to be held accountable for the success of this program. Routine evaluations of the quality of the system, equipment and services are performed to ensure compliance with the terms and conditions of the contract. **Sentinel believes this plan has been successful in making Sentinel programs a success and will follow this plan to measure Sentinel's performance and delivery of services if selected for award.** Sentinel confirms that it has a formal quality control program in place for all department and has attained ISO 9001:2008 certification for manufacturing and Electronic Monitoring Services. Sentinel Offender Services, LLC has implemented processes that have a direct impact to continuous improvement in its Quality Management System. Sentinel's Quality Management System includes the implementation of ISO approved policies and procedures in an effort to achieve the highest possible level of standardization and quality business practice. Sentinel's systems are regularly tested and reviewed to ensure optimum performance standards are met. The tests include all aspects of Sentinel's services, not just functional performance test and monitoring equipment evaluation. Additionally, the results are thoroughly documented, including how cases are being managed and equipment is being issued to participants. Upon contract award, Sentinel will review and modify its Quality Control Plan plan with WSCA and its participating agencies as needed. Sentinel is in a unique position as it stands ready with fully trained, currently employed personnel to provide a full transition and mobilization of this project.
8.5	Monitoring and Evaluation Requirements	The Agency Program Manager or designated staff may perform Agreement compliance reviews during the term of the Agreement. The Agency Program Manager may include periodic review of compliance with contract service delivery.	**Sentinel exceeds this requirement.** Sentinel understands that any participating agency Program Manager or designated staff may perform agreement compliance reviews during the term of the contract including periodic reviews of compliance with contract service delivery. Should issues of non-compliance are identified in any written compliance reports submitted to Sentinel, Sentinel will perform an internal review evaluation of the specific non-compliance and

		The Agency Program Manager will provide written compliance reports to the Contractor. When issues of non-compliance are identified, a written Corrective Action Plan (CAP) will be required of the Vendor. The CAP is to be submitted to the Agency Program Manager within 10 days of receipt of the Agreement compliance review report. Failure to correct deficiencies after thirty (30) days from the date of receipt of the written Agreement compliance review report notating the deficiencies may result in determination of breach of contract and termination of services.	the applicable Standard Operating Procedures. Upon completion of the internal reviews, the Quality Assurance Specialist will ensure the review is sent to the Director of Internal Operations, Chief Operating Officer and appropriate management staff. Management staff will thoroughly discuss the review with any applicable employees to ensure any concerns are appropriately addressed. A Corrective Action Plan will be created and contain notations to summarize the deficiency and be used to document the outcome of the review process. The Corrective Action Plan will be signed by any applicable employee(s) and manager. The Corrective Action Plan will be developed to set clear and realistic goals to correct any deficiencies and enhance the professional development of any reviewed employee. This Corrective Action Plan shall specify, in writing, the corrective measures to be taken with timeframes for resolution included. All Corrective Action Plans will be provided to customers as they are completed, but not more than 10 days of receipt of any compliance review report noting deficiencies. Areas of concern will be reviewed with customer during scheduled quarterly meetings or as requested. Sentinel understands that failure to correct deficiencies after 30 days from the date of receipt of the written agreement compliance review report notating the deficiencies may result in determination of breach of contract and termination of services. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel has established standards that serve as minimum performance criteria throughout the company. These standards will not be enforced as contradictory to the orders of any customers but, rather, to ensure that Sentinel manages the offender monitoring process to the highest possible level of consistent professionalism possible. The Quality Management Team will routinely revise company standards as needed and publish these revisions through memos, emails, checklists and SOP changes. These company standards, regardless of the medium employed for communicating them, will be adhered to as the minimum standards for Sentinel and will be effective immediately as indicated. Along with these Universal Standards a series of checklists and Key Performance Indicator Reports will be available to employees in all department and/or at offices for purposes of self-evaluating their compliance with standards both applicable to the company as well as their department/office. Where local differences may exist between the Universal Standards and the local standards, the highest possible standard that does not conflict with the local

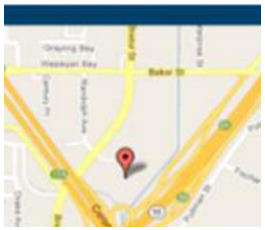
			courts/agencies will be observed. **IMPORTANT SENTINEL ADVANTAGE:** The Chief Operations Officer requires corrective action plans are developed should any **EXTERNAL OR INTERNAL REVIEW** result in deficiencies and follow-up is implemented in each office or department to ensure timely completion of the plan. The Quality Assurance Specialist or designee will address any deficiency in these areas with managerial staff to ensure appropriate action items are listed and followed through. Upon implementation of a corrective action plan, department supervisors and direct responsibility employees meet regularly as determined by the deliverable timelines to ensure that each Key Performance Indicator is successfully achieved. Sentinel conducts these reviews until it is determined that all milestone achievement markers have been fully fulfilled and the overall corrective goal is accomplished ensuring Sentinel quality standards are maintained.
8.6	Background Checks	The Vendor shall conduct Criminal background checks for security purposes on all of its employees. The results of the background checks shall be available for review by the Agency. The MCC Contract Administrator on behalf of the Agency has full discretion to require the Vendor to disqualify, prevent, or remove any of its staff from any work being performed under the Contract upon the report of an unsatisfactory background check.	**Sentinel meets this requirement.** Sentinel understands the importance of having qualified, capable, and trustworthy personnel to handle the needs of a program of this complexity where services are provided to an ethnically, racially, chronologically (age), and economically diversified participant population. Therefore, **Sentinel performs a USIS Widescreen National Criminal/Sex Offender search, state specific misdemeanor and felony checks based on addresses received from their personal Experian TRAC report by social security number, and five-panel drug-testing on its employees before hiring.** Sentinel has in place a company-wide drug-free policy that is clearly outlined prior to hiring with Sentinel as well as clearly posted in common work areas. All employees prior to hiring are subjected to a drug screening, and Sentinel conducts random testing based on reasonable cause. **These results of background checks and/or drug tests can be provided to the agency upon request.** Sentinel understands that Contract Administrator on behalf of the WSCA participating agencies has full discretion to require the awarded vendor to disqualify, prevent, or remove any of its staff from any work being performed under the contract upon the report of an unsatisfactory background check.
8.7	Background Checks	The Vendor shall not offer employment to any individual or assign any individual to work under this Contract, who has not had a background check, conducted and the	**Sentinel meets this requirement.** Sentinel's review process ensures that the candidates meet all background, educational, and experience standards as set forth by contractual obligations. In the event of a misdemeanor, Sentinel can provide a release for the employee to provide permission to release the

		findings of the background check have been determined to be satisfactory.	necessary information to the state regarding the specifics of the employee's event. **Sentinel does not hire persons with felony convictions or misdemeanors with moral turpitude**. All of Sentinel's employees are thoroughly screened to ensure that its employees' backgrounds can be verified and that they can be trusted with access to corrections facilities, court offices, and confidential offender and agency records. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
9.0	**SECTION I Additional Vendor's Equipment and Services**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
9.1		The Vendor may offer additional Equipment and Services. The Vendor should provide list and include a summary of each additional piece of equipment, to include: one device, description, training manuals, functionality, service, and	**Sentinel has proposed the following Optional / Additional Alcohol Monitoring Services and Transdermal Alcohol Monitoring Services:** Optional VI-CAP Patrol™ Alcohol Monitoring Service

		optional pricing. Services may be negotiated based on each user Agency's needs.	Sentinel proposes VI-CAP Patrol™ Alcohol Monitoring as an optional/additional form of Alcohol Monitoring Service. VI-CAP Patrol™ Sentinel is offering WSCA users a choice in Alcohol Monitoring - Sentinel is proposing **VI-CAP Patrol™**, the only fully **supervised** remote alcohol test available in the industry. Through **VI-CAP Patrol™**, WSCA will have the option to conduct random, scheduled and/or on-demand alcohol monitoring tests 24 hours a day. **IMPORTANT SENTINEL ADVANTAGE: VI-CAP Patrol™ meets the WSCA requirements for Alcohol Monitoring Service and is the 11 year incumbent Alcohol Monitoring Service on the existing WSCA contract.** The following list highlights some of the unique features of the proposed **VI-CAP Patrol™** alcohol monitoring service: ▪ **Live Operator Supervision: VI-CAP Patrol™** provides the only supervised remote alcohol test in the industry with live visual verification of the participant. ▪ **Flexible Scheduling Options:** The equipment is flexible enough to test participants by computer generated random tests, monitoring center, agency or officer scheduled testing and on-demand calls to the participant's location. ▪ **Deep Lung Sampling: VI-CAP Patrol™** also includes an Intoxilyzer S-D5 alcohol-testing device designed to take a deep-lung sample and identify the participant's level of intoxication. ▪ **Court Approved:** The equipment provides reliable Breath Alcohol Content (BAC) results. The Optional VI-CAP Patrol™ Alcohol Monitoring Service is included on the Price Worksheets as **an Optional / Additional Alcohol Monitoring Service**. **Optional VI-CAP Patrol™ Mobile Cellular Alcohol Monitoring Service**

Sentinel proposes VI-CAP Patrol™ Mobile, Cellular as an optional/additional form of Alcohol Monitoring Service.

VI-CAP Patrol Mobile



Sentinel is offering WSCA users a choice in alcohol monitoring solutions including mobile, cellular breath alcohol testing. **IMPORTANT SENTINEL ADVANTAGE: VI-CAP Patrol™ Mobile exceeds the WSCA requirements for Alcohol Monitoring Service and is a mobile/cellular enhancement to VI-CAP Patrol™, the 11 year incumbent Alcohol Monitoring Service on the existing WSCA contract.** The following list highlights some of the unique features of the proposed **VI-CAP Patrol™** Mobile alcohol monitoring service:

Advanced Features:

- Mobile Handheld Device Capable of Testing in all Locations
- Immediate Reporting via Cellular
- No Body Worn Equipment
- No Home Equipment, No Need for Home Phone Line
- Deep Lung Sample with w/BAC
- Color Participant Image
- Random or Scheduled Testing
- Tracking of Participant Location at Time of Each Test
- Re-Chargeable Battery, cell phone-like charge concept,
- Officer to Participant Text Communication

Device Testing / Participant Guidance:

- Audible Prompts
- Colored LED Indicators
- Alpha-Numeric Display Prompts
- Test Button
- Front Panel Lights Ensure Quality Photo

Results:

- Email Alerts with BAC Reading
- Color Facial Image from Time of Test
- Web-based Geo-Map of Time of Test Location

The Optional **VI-CAP Patrol™** Mobile Alcohol Monitoring Service is included on the Price Worksheets as an **Optional / Additional Alcohol Monitoring Service**.

Optional Drug Screening Service

Sentinel proposes Drug Screen as an optional/additional form of substance abuse and is listed under the Transdermal Alcohol Monitoring Service.

Sentinel's on-site personnel are certified to provide drug screening services. If requested, Sentinel on-site staff can provide drug screenings based on suspected use or as required by the agency. Sentinel's on-site staff follow agency-specified drug testing procedures with the frequency set forth in the individual offender's case file. Offenders are instructed each visit if they are required to provide a urine sample when they enter the office for meetings.

Currently Sentinel uses an instant five-panel drug detection screen to test for the most commonly abused drugs: THC, Opiates, Amphetamines, Cocaine, and PCP. If the offender's drug of choice is other than those specified in the five-panel test, Sentinel is able to screen for those drugs by ordering drug screen tests for those unique drugs. Sentinel also provides the latest in drug testing options including legally-accepted saliva-based tests that eliminate gender-based collection procedures that can cause collection issues due to offender complaints.

Sentinel considers alcohol and drug use significant indicators of and precursor to criminal offending. Therefore if an offender tests positive:

a) A staff member will notify the offender's agency officer and request direction on how to respond to the violation,
b) The offender is not permitted to interact with other staff members or offenders or attend any service programs, and

			c) If the test is positive for drugs, the sample may be sent to a lab for confirmation of the in-house test results; regardless, d) If the offender drove a motor vehicle to the office, he/she will be instructed not to leave the facility or to drive his/her vehicle, and agency personnel will be contacted immediately. The Optional Drug Screening Service is included on the Price Worksheets as an Optional / Additional Transdermal Alcohol Monitoring Service. **Optional CAM Patrol Plus™ Mobile, Cellular Transdermal Alcohol Monitoring Service** Sentinel proposes **CAM Patrol Plus™** as an optional/additional form of Transdermal Alcohol Monitoring Service. Sentinel is offering WSCA users a choice in transdermal alcohol monitoring solutions including **CAM Patrol Plus™**. **CAM Patrol Plus™** transdermal alcohol monitoring device, which incorporates a small lightweight transmitter bracelet with built-in alcohol sensor to detect traces of Ethanol in a person based on their alcohol consumption. **IMPORTANT SENTINEL ADVANTAGE: The proposed solution is unique in that it also incorporates GPS tracking and location based monitoring and has capability for 2-way voice communication.** The **CAM Patrol Plus™** transdermal alcohol monitoring and location-based tracking solution provides the following unique features and benefits: ▪ **Totally Wireless Solution:** The **CAM Patrol Plus™** unique patented design allows for constant communications with the transmitter and ability to communicate with monitoring center through the wireless network. ▪ **Alcohol Test Results Every 15 Minutes:** The **CAM Patrol Plus™** has the ability to detect traces of Ethanol in a person based on their alcohol consumption and to communicate alcohol test results to the monitoring center every 15 minutes providing the agency the ability to respond immediately to an alcohol violation as it happens rather than after the fact as the agency doesn't have to wait until a participant gets home for the unit download the data.

- **Reliable Cellular Coverage for Immediate Reporting:** As the normal use of cellular technology is increasing across the United States, it has become more and more common for participants to not have landline telephone communications in their home. As such, leading electronic monitoring companies have adapted to use cellular communications for reporting of monitoring data. Sentinel is in a unique position to offer transdermal alcohol monitoring using multiple cellular carrier option including Nextel, Sprint and Verizon.
- **Integrated Continuous Active GPS:** **The CAM Patrol Plus™ incorporates GPS tracking and location based monitoring rather than simple house arrest technology and provides for the ability to set inclusion zones and exclusion zones to track program participants throughout the community providing an increased level of monitoring above traditional house arrest technology allowing the agency to know where a participant is, not just whether or not they are not at home.**
- **Adjustable Location Points:** The **CAM Patrol Plus™** solution's GPS tracking unit handset can send GPS location points as frequently as every 60 seconds regardless of violation status and provides the ability of the agency to customize the frequency setting for each participant's handset.
- **Flexible and User Friendly Web–Interface:** The **CAM Patrol Plus™** solution incorporates a web-based Internet information exchange, the View User Interface (VUI), to configure the alcohol sensors remotely, for accessing participant alcohol levels and location maps including satellite images for more precise, pinpoint GPS locations and to run monitoring reports.
- **Automatic Alerts and Notifications:** The **CAM Patrol Plus™** solution offers automated alerts for both zone and alcohol violations.

			Additionally, the monitoring center operates 24 hours a day 365 days per year and is always there to work with agency staff regarding alcohol readings and alarm resolutions. ▪ **Two-Way Voice Communications: The CAM Patrol Plus™ tracking handset provides the ability to communicate directly with any participant at any time through two-way voice communications**. ▪ **Mobile Monitoring Capability:** Agency can monitor participant activity using Mobile Software on a Blackberry. **Also unique to the CAM Patrol Plus™ technology, the overall solution does not require several cumbersome or expensive features required by other vendors including:** ▪ **No Receiver in the Home:** The **CAM Patrol Plus™** technology solution does not require a receiver unit to be installed or maintained in the participant's residence. ▪ **No Need for Landline Communications:** The **CAM Patrol Plus™** technology solution does not require a standard pulse or touch-tone telephone to be installed at the participant's residence. ▪ **No Need for Downloads:** The need for downloads is eliminated with this solution because the **CAM Patrol Plus™** bracelet and handset **continuously transmits** via the cellular provider, the **GPS location** and **alcohol level** data, to the monitoring center. The Optional **CAM Patrol Plus™** Transdermal Monitoring Service is included on the Price Worksheets as **an Optional / Additional Transdermal Alcohol Monitoring Service**.
10a.0	**SECTION J ALCOHOL MONITORING EQUIPMENT AND SERVICE** **Vendor Provided Offender Services - for single body-attached devise with receiver**		
Item	**Description**		**Describe how Vendor meets or exceeds specifications**
10a.1	The government entity may choose to provide the contractor with reasonable office space onsite within the government agencies office locations.		**Sentinel exceeds this requirement.** Sentinel understands each user agency may choose to provide the contractor with reasonable office space onsite within the government agencies office locations. Additionally, dependent on program size and participant numbers, Sentinel may be willing to open a separate local office to facilitate the preferred optional service offerings described in this proposal. Should a full time office to be opened within and local staff be hired and trained, this would allow Sentinel to expand its service offering to include

		additional full-service program options. Once established this location could be utilized by county agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand these programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates. Sentinel understands the need for full service programs nationwide and believes that many WSCA participating agencies are prime candidates for such programs.
10a.2	Each entity will maintain its own computers, software, and internet service for exchanging information.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for the maintenance of agency-owned computers, software and Internet service for exchanging information.
10a.3	The government entity will maintain complete responsibility for program management services not specifically listed	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all program management services not specifically listed in this section of the RFP 00212, Electronic Monitoring of Offenders.
10a.4	The government agency will be responsible for all referrals of all new offenders to the program	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all responsible for all referrals of all new offenders to their programs.
10a.5	Prior to any referral the government entity will ensure that the subject has a home phone or identifies the need of a cellular service monitoring unit.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for ensuring that all offenders referred to the program have an operational home phone or identifies the need of a cellular service monitoring unit.
10a.6	Offenders should have an ability to pay for enrollment and services provided by the contractor.	**Sentinel exceeds this requirement.** Each offender will have the ability to pay for enrollment and services provided Sentinel. Sentinel understands that the objectives of offender-funded programs are to provide accountability to the participants through provision of selected court-referred programs and **ensuring each adult, with a demonstrated ability to pay, is responsible for payment for monitoring**. An important segment of the Intake and Orientation Meeting are the financial assessment and fee payments. Using the approved fee schedules as set forth in the pricing section based on the financial assessment process detailed as the response to specification 10.a.7, Sentinel will review the costs of the program, ensure all required payments have been made and receive any payments scheduled at this time. Currently, Sentinel provides collection of fees from defendants and daily reporting to the court, **specifically for more than 45,000 offender-paid participants.**

Sentinel pioneered the concept of offender-funded services and is highly experienced in incorporating a sliding fee scale model including the provision of services to participants that are deemed indigent.

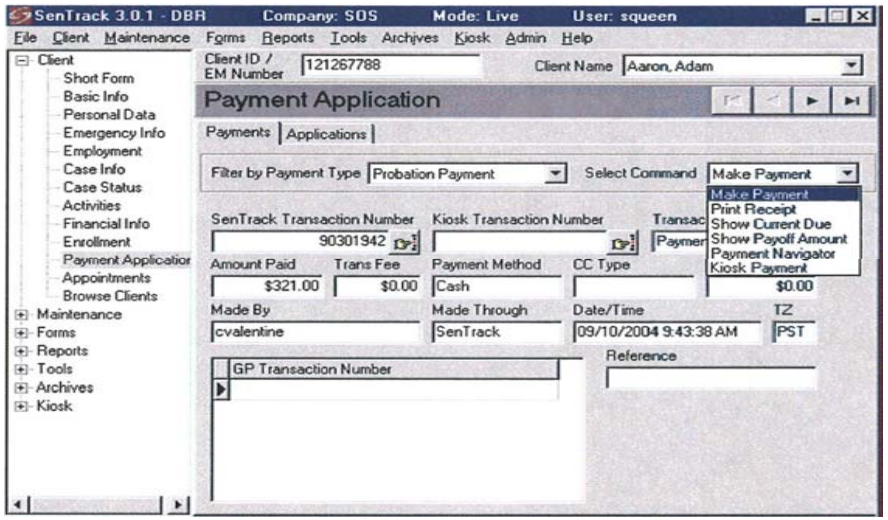
For those participants that show inability to pay full program fees after all the above elements have been considered, Sentinel will offer a discounted rate off of the full program fees to the participant. The rate will be based on an assessment of the participant's ability to pay. Should the participant not agree with the assessment and discounted rate, Sentinel will provide its finding to the participating agency/courts for recommendations on how to proceed.

Sentinel will use the following strategies to ensure successful collections:

- Sentinel local staff (if available) will address the importance of keeping current with all program fees and each participant will be required to sign an agreement which outlines program fees and how and when program fees are to be submitted.
- Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc.
- **IMPORTANT SENTINEL ADVANTAGE:** Sentinel can also offer an optional on-site Kiosk that will allow offenders to pay monitoring fees electronically. **PLEASE NOTE:** Through this kiosk, Sentinel can offer an optional service to allow offenders to pay other fees owed to the participating agency or other county/city/state

Kiosk

		agencies such as parking tickets, court fines or restitution. ▪ Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason. ▪ Sentinel local staff (if available) will promptly follow-up on missed or partial payments. ▪ Sentinel will reassess the financial conditions for those participants who have experienced a sudden change in income in order to reevaluate if the participant's ability or inability to pay the established and agreed upon program fees warrant a reduction in fees. ▪ Sentinel will use collection agencies if needed in order to recoup established program fees. ▪ Sentinel will provide monthly reports to the participating agency and/or courts that provide details on fees collected from the offender funded program. ▪ Sentinel will also provide a report that will detail Sentinel's efforts for collecting fees from delinquent participants. ▪ Sentinel will immediately advise the participating agency and/or courts on any offender's refusal to pay program fees to see about having the participant removed from the program. **IMPORTANT SENTINEL ADVANTAGE:** All participant payments made to Sentinel are processed through Sentinel's proprietary SenTrack software and made available to the participating agencies or courts via this automated software interface and in hard copy reports/invoices. Within this system, Sentinel will track the progress of participant payments as well as alcohol test results, drug screens, report dates, and other court order conditions that may be required by or beyond the Scope of Work for this program. All activity is automatically time- and date-stamped within the software for chronological integrity purposes. SenTrack allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software. The following screen image provides a quick glance showing the thorough nature and ease-of-use of the SenTrack case management software. Sentinel has provided a screen image of the payment application illustrating some of the highlights of software.

		CONFIDENTIAL  **Screen Image of "Payment Application Mode" within SenTrack:** SenTrack's Automated Payment Application function accurately accounts for all defendant payments
10a.7	Contractor will make arrangements to create a fee payment assessment whereby the cost of the program to offenders will be set on a mutually agreed upon schedule based on monthly earnings of an offender.	**Sentinel exceeds this requirement.** Sentinel recognizes the budget concerns facing agencies nationwide. The challenges of providing thorough supervision within budget constraints have resulted in many localities charging the cost of electronic monitoring and re-entry programs back to participants in an effort to stretch budgeted electronic monitoring dollars. More importantly, Sentinel's experience with offender-paid programs indicates that some level of payment for service, regardless of the amount, is a strong enhancement in the performance of the participant in the program, resulting in a substantial reduction in recidivism. **Sentinel is experienced in offender-funded programs and has processes and systems in place that presently charge thousands of participants nationwide for the cost of their own electronic supervision** allowing agencies to save time and valuable resources by relieving the internal administrative burden of collecting, tracking and reporting offender fees. Sentinel has always been an innovator in its industry and in fact **pioneered the offender-funded program model** in response to changing industry needs. This

		model allows Sentinel to provide all of its monitoring services at little or no cost to the agencies, **thereby saving correctional agencies tens-of-millions-of-dollars in jail cost and monitoring fee avoidance**. Offender-funded electronic monitoring is Sentinel's core business operation and with no impact on operational budgets to fund these monitoring programs, agencies were able to further expand the programs without requiring additional funds to pay for monitoring services. This is a program model that Sentinel has used with great success since 1992, and **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers. **When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services.** Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors: (1) Present financial position. (2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position. (3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program. (4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision. **Sentinel is the most experienced in the industry in managing offender funded programs based on a sliding-scale fee structure for those participants identified as indigent.** Sentinel has the ability to offer a graduated fee scale available to the WSCA participating agencies for determination of reduced fees to be collected for an indigent participating offender where some participants will be able to pay the full program fees while some will only be able to pay a portion of the daily fees or no fees at all. As part Sentinel's offender-funded program,

		Sentinel will collect fees from participants on a flat fee or sliding scale basis based on the following Offender Funded Program on the following characteristics: ▪ Minimum average of 100 active participant per installation area ▪ Average participant term on monitoring of 30 days ▪ 75 square mile installation area ▪ One Sentinel Installer/Case Manager per installation area ▪ Participants maintain a two-week advance payment ▪ 75% of participants willing to report to local Sentinel office for: ✓ Initial activation/orientation ✓ Equipment return ✓ Offender-fee payments ▪ Equipment/Monitoring/Notification consistent with that proposed for WSCA ▪ Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment. Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variances with any WSCA end user agency for Offender Funded Program Services. **Sentinel has a current financial assessment form already in use at other various agencies as well as proven invoicing and fee collections procedures in place to ensure program success right out of the gait should any agency choose to utilize these services.** The methodology used by Sentinel for determining offender-funded fees is based on Sentinel's extensive experience, performance and success in providing these services to other criminal justice entities. Sentinel will conduct a financial assessment for every offender who has been determined eligible for the program by the participating agencies/courts. Sentinel's financial assessment process takes into consideration the participant's current and future financial status when determining a participant's ability or inability to pay the daily maximum as established in the sliding fee scale table that is based on the adjusted annual household income.
10a.8	The contractor will activate and install equipment on offenders and	**Sentinel exceeds this requirement.** During the Intake and/or Orientation

	orientate offenders on home equipment placement or transdermal unit connection and care.	meeting, Sentinel's Project Director/Case Manager(s) will install and activate all necessary alcohol monitoring/electronic monitoring equipment on the participant or in the participant's home. Sentinel can offer a full continuum of electronic/alcohol monitoring equipment to monitor and verify that program participants abstain from alcohol-use as well as remain at home/work during specified time periods. During the Intake and/or Orientation meeting, Sentinel will also review written orientation manuals describing the operation and care of the monitoring equipment that can be distributed to participants after device installations. Additionally during this meeting, Sentinel's Project Director/Case Manager(s) will collect and verify all of the necessary participant documentation and information to verify the participant's employment, community restitution, treatment classes, religious activities, funeral services, medical appointments and any other activities the person participates in on an on-going basis. In addition to confirming the participant's information, all permitted activities and required verification/ documentation including reasons for possible termination from the program would be explained to the participant so that there were no misunderstandings. Additionally, during this meeting Sentinel will: ▪ Obtain a copy of the Pre-conviction or conviction from the participant, jail and/or court ▪ Verify participant's name, date of birth, home address, telephone number, race and family details ▪ Verify court details including docket number, assigned judge, date of the court order, anticipated date of execution of sentence and restitution requirements ▪ Capture participant photograph and signature ▪ Obtain signature of participant consent for the Authorization for Information Release (if required) ▪ Complete a financial assessment of the participant to determine indigent status (if required) ▪ Complete a risk/need assessment to determine the participant's Case Plan (if full-service option selected)

		▪ Inform the participant of the days they are required to report into the office for face-to-face meetings ▪ Review required restitution and fee payments
10a.9	Offenders will be responsible for the cost of lost, damaged, or stolen equipment.	**Sentinel meets this requirement.** Sentinel understands that program participants will be responsible for the cost of lost, damaged, or stolen equipment. Sentinel will directly bill all participants for equipment that was lost, stolen damaged. Based upon Sentinel' experience in other contracts, Sentinel has found a few points essential to improved management of equipment inventory and loss, damaged or stolen equipment. This includes increased emphasis to not remove the transmitter until all pieces of equipment provided to the participant are together in the same place, either at the participant's home or the Sentinel office. Sentinel would request ongoing coordination with the participating agencies for participants to return equipment to Sentinel local office.
10a.10	**The contractor should provide limited case management to include:**	**Sentinel exceeds this requirement. Sentinel is proposing several value-added options to help elevate the burden of routine program management, installation/retrieval service, compliance monitoring, inventory management and fee collections from WSCA participating agency employees allowing officers more time to manage violations and provide needed case management to its offender population.** Sentinel provides options for both **limited or full-service case management** in addition to installation and retrieval services will allow both agencies to simply refer participants to Sentinel and receive violation notifications for all program participants through immediate automated or manual notifications. Sentinel is committed to providing a continuum of case management operations to WSCA participating agencies that would allow for Sentinel staff to be located on-site for program operation. In addition to the standard requirements of this RFP, Sentinel is also proposing a completely offender funded program that would allow participating agencies to avoid collecting fees directly from program participants. Sentinel's case management model would allow for a full time office to be opened and local staff to be hired and trained. Once established this location could be utilized by participating agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand your programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates.

		Case supervision services are an integral component of the judicial process; therefore selecting the correct service provider is a critical decision. **Sentinel currently provides case management services to more than 100 programs from more than 50 locally-based offices across the country.** In these programs, Sentinel's staff monitors compliance to the court-ordered conditions with court orders via regularly scheduled meetings with each participant, addresses all issues of non-compliance, and reports continued non-compliance to the supervising agencies for resolution. Sentinel maintains individual case files on all participants for review by the court or its designees and in order to provide documentation for use in enforcement or revocation matters. Additionally, Sentinel has extensive experience customizing programs at the local level and currently **works directly with over 95 judges**. Through these programs, Sentinel's supervision services staff conducts more than **55,000 face-to-face defendant contacts a month**. Additionally, Sentinel understands the importance of expert court testimony and on a daily basis Sentinel has as many as **50 employees a day working in court rooms** nationwide testifying regarding participant activity. **This level of experience is difficult to replicate by any vendor and Sentinel is confident that its proposed program can exceed the court's expectations.** Sentinel has extensive experience provide the following staff members to programs utilizing its limited- or full-service case management services: **Program Director:** Dependent on the size of the specific program, Sentinel may employ a Program Director as the lead contact for the daily operation of the program and handle any court requests. The candidate will hold at minimum a Bachelor's Degree in social work or counseling and have counseling or social work experience with participants. This person's duties will include: ▪ Daily reconciliation of all payments received ▪ Supervision of all Sentinel office staff ▪ Quality assurance audits and reviews of supervision methodologies ▪ Oversee all contacts with victims ▪ Investigate all participants grievances ▪ Daily liaison for court personnel ▪ Court representative for any proceedings for participants ▪ Steering committee representative for Sentinel with court/agency

		personnel **Case Manager(s):** Case Manager candidates will also hold at minimum of a Bachelor's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include: ▪ Adhering to Sentinel's Case Management Model including performing (1) Assessment, (2) Interpretation, (3) Case Planning, (4) Ensuring the Delivery of Services and (5) Evaluating Performance ▪ Explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature ▪ Create and maintain files on all participants referred to the program ▪ Process all payments ▪ Communication with court personnel if there are any inquiries on a specific participants ▪ Perform notifications of program completions/non-compliance **Administrative Assistant:** Depending on the size of the specific programs and the volume of tasks placed on an office providing this type of service to a participant population, an Administrative Assistant maybe needed. This person will: ▪ Handle all calls received at the office ▪ Provide assistance to the Program Director and Case Manager(s) as needed ▪ Assist with performing any required transmission of reports ▪ General office tasks **IMPORTANT SENTINEL ADVANTAGE:** Sentinel has helped pioneer the concept of opening local, community-based "Success Centers" where probationers/defendants/parolees can participate in electronic monitoring programs and optionally receive assistance with job placement, address drug addiction, as well as participate in cognitive skills classes, anger management and other developmental programs. Using this model, Sentinel can work directly with the participating agency and the courts to develop additional programs at its Success Center to help reduce recidivism **AT NO COST TO THE AGENCY**. Sentinel's basic business model rests on proven research that has shown that heavier punishment and long terms of incarceration or probation are not lasting answers to stem criminal behavior. Rehabilitation-oriented

		programs and defendant accountability, combined with community-based intervention and support, is the more sensible way to tackle this complex issue. Should participating agencies elect to utilize the Success Center Model, Sentinel will additionally provide the following staff members: **Program Specialist(s):** Program Specialist candidates will hold at minimum a Master's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include: ▪ Delivery of daily classes based on Diversion Orders or needs assessments ▪ Communication with the Project Director/Case Manager(s) regarding each defendants progress regarding his or her Case Plan ▪ Maintaining current on all applicable laws and changing regulations for class delivery
10a.11	a. Contractor will coordinate offender (in person) reporting on a schedule agreed upon by both parties	**Sentinel meets this requirement.** Sentinel Program Directors/Case Managers will be responsible for explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature. During Intake and Orientation, Sentinel will coordinate an agreed upon in-person reporting schedule with the participant based on the participants risk level assigned by the court and/or determined through Sentinel's risk assessment tools. Sentinel is capable and willing to provide monthly, bi-monthly, weekly and/or bi-weekly face-to-face offender compliance meetings in addition to daily monitoring of compliance or violation and the reporting of all participant activities. Please note that Sentinel understands that one of the main segments of an active case management program is the ability to verify that the offenders are abiding by all program regulations. Sentinel's program model is designed so that its program directors/case managers meet regularly with the program participants to review all of their activities and their activity documentation. **Sentinel has**

		been successfully providing this exact program model to Los Angeles County since the early 1990's.
10a.12	b. The contractor will confirm the employment status of the offender and financial status.	**Sentinel exceeds this requirement.** Sentinel will verify and confirm the validity of all pre-approved locations including work, school, college, counseling, AA/NA, victim awareness or other program classes and capture teacher/supervisor information for additional follow-up. **When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services.** Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors: (1) Present financial position. (2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position. (3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program. (4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision. **IMPORTANT SENTINEL ADVANTAGE:** During the course of any participant's monitoring, Sentinel will continue to confirm the on-going employment status of the participant and/or any changes financial status either during scheduled meetings or random spot checks/call to the place of employment.
10a.13	c. The contractor will collect fees from the offender and will provide notices to the government agency on delinquent payments	**Sentinel exceeds this requirement. Sentinel will be responsible for invoicing and the collection of fees from all participants.** Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender

		payments, Sentinel will offer follow-up call-center intervention to remind offenders of pending and/or over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc. Additionally, Sentinel local staff will promptly follow-up on missed or partial payments. Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason. **Additionally, should any participant become delinquent on payments, Sentinel will provide a delinquency notice to both the participant and participating agency informing them of the delinquency, detailing Sentinel's efforts for collecting fees from delinquent participants and Sentinel's recommended course of action regarding the participants continued monitoring.** Sentinel will also provide regularly scheduled (i.e. monthly, quarterly, etc.) reports to the participating agency and/or courts that provide details on all fees collected/uncollected from the offender-funded program. Sentinel **has monitored more than 1 million offender-paid electronic monitoring participants**. **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has directly collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers.
10a.14	d. The contractor will review offender curfew activity from the time since the offender last reported.	**Sentinel meets this requirement.** During each scheduled compliance review, each participant will provide activity documentation to verify their whereabouts in the community since their previous compliance appointment. Sentinel's project director/case managers will also carefully review the daily alcohol monitoring reports as well as any curfew reports and/or GPS tracking maps that are available to verify that the offenders actually attended the activities they are permitted to by the participating agency and/or courts.
10a.15	e. The contractor will review monitoring /tracking activity with the offender and provide the government agency with exception reports for program violations.	**Sentinel meets this requirement.** During each scheduled compliance review, each participant will provide activity documentation to verify their whereabouts in the community since their previous compliance appointment. Sentinel's project director/case managers will also carefully review the daily alcohol monitoring reports as well as any curfew reports and/or GPS tracking maps that are available to verify that the offenders actually attended the activities they are

		permitted to by the participating agency and/or courts. Any violations, inconsistencies or incorrect documentation will result in a Non Compliance Report being issued to the participant and provided to the participating agency for review/enforcement.
10a.16	f. The contractor's case management activities shall be documented in the contractor's caseload management software and accessible to the government entity 24/7.	**Sentinel exceeds this requirement.** Sentinel designed its proprietary, web accessible case management software, SenTrack, specifically for use in the offender services arena. Employing SenTrack allows **real-time, on-line web accessibility** to participant case information and reports for Sentinel employees **and** authorized participant agency and/or court personnel. As the SenTrack case management software is an in-house concept and design, SenTrack is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support and recommends all participating stakeholders have access to the SenTrack software for program review and oversight.** **IMPORTANT SENTINEL ADVANTAGE:** SenTrack allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software. Sentinel catapulted the speed, capacity and capabilities of case management software through the development of the SenTrack SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective. **This translates into the ability to modify or develop new software variations as may be needed for the agency directly, in house, without having to utilize outside vendors which may bring data security concerns to the agency. Only Sentinel personnel would have access to the confidential participant data and the development of any new application.** Sentinel's SenTrack case management software incorporates all of the technology offered by Sentinel. The software is fully integrated in every Sentinel branch office and has become the foundation from which Sentinel serves its customers. Highlights of the SenTrack case management software include: ▪ Internet accessibility; available 24 hours a day to any Sentinel customer ▪ All client obligations to the court are tracked (courses, fines, drug

		screens, community service, restitution, demographics etc.) ▪ Real-time communication with Kiosks ▪ On-line payment acceptance ▪ Proprietary Case Management Software; 100% in-house support and customization available ▪ Over 150 available reports ▪ Customized reports provided at **no cost** ▪ Currently services more than 200 agencies and over 45,000 offender-paid participants ▪ Able to capture photo images as required ▪ Fully redundant and supported by continuous operation monitoring center designed to Underwriters Laboratory specifications ▪ Internal audit tools track all changes ▪ Unlimited query capabilities for detailed statistical reporting **The SenTrack system is completely customizable and currently provides more than 150 different types of case management and financial reports. Through the ability to customize the system, SenTrack has made it possible for judges to have the reports they want in the format they desire.** **IMPORTANT SENTINEL ADVANTAGE:** Due to Sentinel's extensive experience in providing case management and supervision programs, Sentinel has created and utilized its proprietary database system to manage all caseloads including compliance to the program's regulations. Along with status reports that Sentinel can provide to update the participant's program status to the participating agency and/or court staff, Sentinel will also create non-compliance reports (NCR). Sentinel's non-compliance reports have easy "check-off boxes" that identify specific instances of non-compliance. The advanced Sentinel SenTrack system also allows for an on-going tally system showing the number of NCR's issued, along with the information as to how many remain "open" and how many have been resolved. This supplementary information is essential to agency staff trying to make a decision as to the participant's overall program compliance.

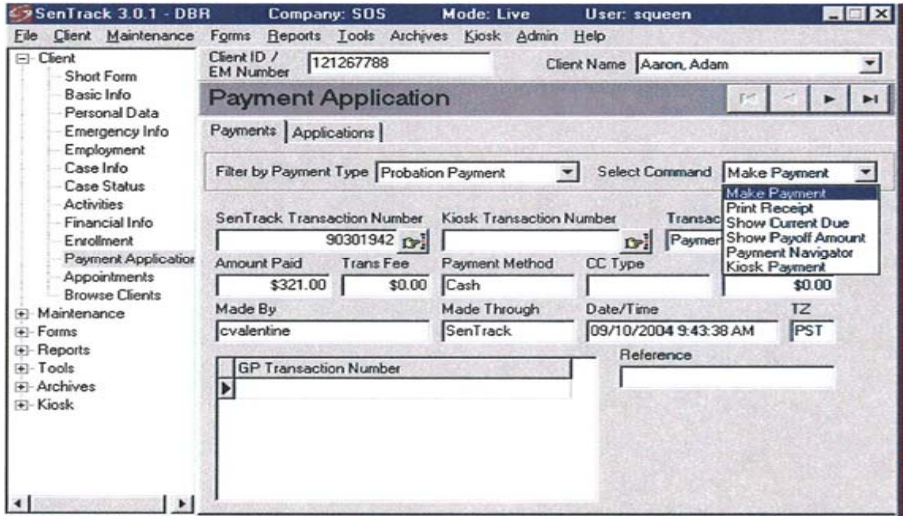
		CONFIDENTIAL **Non-Compliance Report Screen in SenTrack**: In the event that a participant does not comply with the regulations and conditions of the program, Sentinel staff will generate a non-compliance report that will include a narrative explaining the details of the situation, along with a quick-reference "check-off" box choice as illustrated
10b.0	**SECTION J ALCOHOL MONITORING TRANSDERMAL EQUIPMENT AND SERVICE** **Vendor Provided Offender Services for Alcohol Monitoring Transdermal Equipment and Service**	
Item	**Description**	**Describe how Vendor meets or exceeds specifications**
10b.1	The government entity may choose to provide the contractor with reasonable office space onsite within the government agencies office locations.	**Sentinel exceeds this requirement.** Sentinel understands each user agency may choose to provide the contractor with reasonable office space onsite within the government agencies office locations. Additionally, dependent on program size and participant numbers, Sentinel may be willing to open a separate local office to facilitate the preferred optional service offerings described in this proposal. Should a full time office to be opened within and local staff be hired and trained, this would allow Sentinel to expand its service offering to include additional full-service program options. Once established this location could be utilized by county agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand these programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates. Sentinel understands the need for full service programs nationwide and believes that many WSCA participating agencies are prime candidates for such programs.
10b.2	Each entity will maintain its own computers, software, and internet	**Sentinel meets this requirement.** Sentinel understands each user agency will

	service for exchanging information.	be responsible for the maintenance of agency-owned computers, software and Internet service for exchanging information.
10b.3	The government entity will maintain complete responsibility for program management services not specifically listed	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all program management services not specifically listed in this section of the RFP 00212, Electronic Monitoring of Offenders.
10b.4	The government agency will be responsible for all referrals of all new offenders to the program	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for all responsible for all referrals of all new offenders to their programs.
10b.5	Prior to any referral the government entity will ensure that the subject has a home phone or identifies the need of a cellular service monitoring unit.	**Sentinel meets this requirement.** Sentinel understands each user agency will be responsible for ensuring that all offenders referred to the program have an operational home phone or identifies the need of a cellular service monitoring unit.
10b.6	Offenders should have an ability to pay for enrollment and services provided by the contractor.	**Sentinel exceeds this requirement.** Each offender will have the ability to pay for enrollment and services provided Sentinel. Sentinel understands that the objectives of offender-funded programs are to provide accountability to the participants through provision of selected court-referred programs and **ensuring each adult, with a demonstrated ability to pay, is responsible for payment for monitoring**. An important segment of the Intake and Orientation Meeting are the financial assessment and fee payments. Using the approved fee schedules as set forth in the pricing section based on the financial assessment process detailed as the response to specification 10.b.7, Sentinel will review the costs of the program, ensure all required payments have been made and receive any payments scheduled at this time. Currently, Sentinel provides collection of fees from defendants and daily reporting to the court, **specifically for more than 45,000 offender-paid participants.** Sentinel pioneered the concept of offender-funded services and is highly experienced in incorporating a sliding fee scale model including the provision of services to participants that are deemed indigent. For those participants that show inability to pay full program fees after all the above elements have been considered, Sentinel will offer a discounted rate off of the full program fees to the participant. The rate will be based on an assessment of the participant's ability to pay. Should the participant not agree with the assessment and discounted rate, Sentinel will provide its finding to the participating agency/courts for recommendations on how to proceed. **Sentinel will use the following strategies to ensure successful collections:**

- Sentinel local staff (if available) will address the importance of keeping current with all program fees and each participant will be required to sign an agreement which outlines program fees and how and when program fees are to be submitted.
- Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc.
- **IMPORTANT SENTINEL ADVANTAGE:** Sentinel can also offer an optional on-site Kiosk that will allow offenders to pay monitoring fees electronically. **PLEASE NOTE:** Through this kiosk, Sentinel can offer an optional service to allow offenders to pay other fees owed to the participating agency or other county/city/state agencies such as parking tickets, court fines or restitution.

- Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason.
- Sentinel local staff (if available) will promptly follow-up on missed or partial payments.
- Sentinel will reassess the financial conditions for those participants who have experienced a sudden change in income in order to reevaluate if the participant's ability or inability to pay the established and agreed upon program fees warrant a reduction in fees.
- Sentinel will use collection agencies if needed in order to recoup established program fees.

		▪ Sentinel will provide monthly reports to the participating agency and/or courts that provide details on fees collected from the offender funded program. ▪ Sentinel will also provide a report that will detail Sentinel's efforts for collecting fees from delinquent participants. ▪ Sentinel will immediately advise the participating agency and/or courts on any offender's refusal to pay program fees to see about having the participant removed from the program. **IMPORTANT SENTINEL ADVANTAGE:** All participant payments made to Sentinel are processed through Sentinel's proprietary SenTrack software and made available to the participating agencies or courts via this automated software interface and in hard copy reports/invoices. Within this system, Sentinel will track the progress of participant payments as well as alcohol test results, drug screens, report dates, and other court order conditions that may be required by or beyond the Scope of Work for this program. All activity is automatically time- and date-stamped within the software for chronological integrity purposes. SenTrack allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software. The following screen image provides a quick glance showing the thorough nature and ease-of-use of the SenTrack case management software. Sentinel has provided a screen image of the payment application illustrating some of the highlights of software.

		CONFIDENTIAL  **Screen Image of "Payment Application Mode" within SenTrack:** SenTrack's Automated Payment Application function
10b.7	Contractor will make arrangements to create a fee payment assessment whereby the cost of the program to offenders will be set on a mutually agreed upon schedule based on monthly earnings of an offender.	**Sentinel exceeds this requirement.** Sentinel recognizes the budget concerns facing agencies nationwide. The challenges of providing thorough supervision within budget constraints have resulted in many localities charging the cost of electronic monitoring and re-entry programs back to participants in an effort to stretch budgeted electronic monitoring dollars. More importantly, Sentinel's experience with offender-paid programs indicates that some level of payment for service, regardless of the amount, is a strong enhancement in the performance of the participant in the program, resulting in a substantial reduction in recidivism. **Sentinel is experienced in offender-funded programs and has processes and systems in place that presently charge thousands of participants nationwide for the cost of their own electronic supervision** allowing agencies to save time and valuable resources by relieving the internal administrative burden of collecting, tracking and reporting offender fees. Sentinel has always been an innovator in its industry and in fact **pioneered the offender-funded program model** in response to changing industry needs. This model allows Sentinel to provide all of its monitoring services at little or no

		cost to the agencies, **thereby saving correctional agencies tens-of-millions-of-dollars in jail cost and monitoring fee avoidance**. Offender-funded electronic monitoring is Sentinel's core business operation and with no impact on operational budgets to fund these monitoring programs, agencies were able to further expand the programs without requiring additional funds to pay for monitoring services. This is a program model that Sentinel has used with great success since 1992, and **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers. **When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services.** Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors: (1) Present financial position. (2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position. (3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program. (4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision. **Sentinel is the most experienced in the industry in managing offender funded programs based on a sliding-scale fee structure for those participants identified as indigent.** Sentinel has the ability to offer a graduated fee scale available to the WSCA participating agencies for determination of reduced fees to be collected for an indigent participating offender where some participants will be able to pay the full program fees while some will only be able to pay a portion of the daily fees or no fees at all. As part Sentinel's offender-funded program, Sentinel completes a financial assessment of participants and provides a reduction or waiver of up to 5% of the

		total population who are financially unable to pay the already established rates. Sentinel will collect fees from participants on a flat fee or sliding scale basis based on the following Offender Funded Program on the following characteristics: ▪ Minimum average of 100 active participant per installation area ▪ Average participant term on monitoring of 30 days ▪ 75 square mile installation area ▪ One Sentinel Installer/Case Manager per installation area ▪ Participants maintain a two-week advance payment ▪ 75% of participants willing to report to local Sentinel office for: ✓ Initial activation/orientation ✓ Equipment return ✓ Offender-fee payments ▪ Equipment/Monitoring/Notification consistent with that proposed for WSCA ▪ Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment. Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variances with any WSCA end user agency for Offender Funded Program Services. **Sentinel has a current financial assessment procedure and participant forms already in use at other various agencies as well as proven invoicing and fee collections procedures in place to ensure program success right out of the gait should any agency choose to utilize these services.** The methodology used by Sentinel for determining offender-funded fees is based on Sentinel's extensive experience, performance and success in providing these services to other criminal justice entities. Sentinel will conduct a financial assessment for every offender who has been determined eligible for the program by the participating agencies/courts. Sentinel's financial assessment process takes into consideration the participant's current and future financial status when determining a participant's ability or inability to pay the daily maximum as established in the sliding fee scale table that is based on the adjusted annual household income.

10b.8	The contractor will activate and install equipment on offenders and orientate offenders on home equipment placement or transdermal unit connection and care.	**Sentinel exceeds this requirement.** During the Intake and/or Orientation meeting, Sentinel's Project Director/Case Manager(s) will install and activate all necessary alcohol monitoring/electronic monitoring equipment on the participant or in the participant's home. Sentinel can offer a full continuum of electronic/alcohol monitoring equipment to monitor and verify that program participants abstain from alcohol-use as well as remain at home/work during specified time periods. During the Intake and/or Orientation meeting, Sentinel will also review written orientation manuals describing the operation and care of the monitoring equipment that can be distributed to participants after device installations. Additionally during this meeting, Sentinel's Project Director/Case Manager(s) will collect and verify all of the necessary participant documentation and information to verify the participant's employment, community restitution, treatment classes, religious activities, funeral services, medical appointments and any other activities the person participates in on an on-going basis. In addition to confirming the participant's information, all permitted activities and required verification/ documentation including reasons for possible termination from the program would be explained to the participant so that there were no misunderstandings. Additionally, during this meeting Sentinel will: ▪ Obtain a copy of the Pre-conviction or conviction from the participant, jail and/or court ▪ Verify participant's name, date of birth, home address, telephone number, race and family details ▪ Verify court details including docket number, assigned judge, date of the court order, anticipated date of execution of sentence and restitution requirements ▪ Capture participant photograph and signature ▪ Obtain signature of participant consent for the Authorization for Information Release (if required) ▪ Complete a financial assessment of the participant to determine indigent status (if required)

		▪ Complete a risk/need assessment to determine the participant's Case Plan (if full-service option selected) ▪ Inform the participant of the days they are required to report into the office for face-to-face meetings ▪ Review required restitution and fee payments
10b.9	Offenders will be responsible for the cost of lost, damaged, or stolen equipment.	**Sentinel meets this requirement.** Sentinel understands that program participants will be responsible for the cost of lost, damaged, or stolen equipment. Sentinel will directly bill all participants for equipment that was lost, stolen damaged. Based upon Sentinel' experience in other contracts, Sentinel has found a few points essential to improved management of equipment inventory and loss, damaged or stolen equipment. This includes increased emphasis to not remove the transmitter until all pieces of equipment provided to the participant are together in the same place, either at the participant's home or the Sentinel office. Sentinel would request ongoing coordination with the participating agencies for participants to return equipment to Sentinel local office.
10b.10	**The contractor should provide limited case management to include:**	**Sentinel exceeds this requirement. Sentinel is proposing several value-added options to help elevate the burden of routine program management, installation/retrieval service, compliance monitoring, inventory management and fee collections from WSCA participating agency employees allowing officers more time to manage violations and provide needed case management to its offender population.** Sentinel provides options for both **limited or full-service case management** in addition to installation and retrieval services will allow both agencies to simply refer participants to Sentinel and receive violation notifications for all program participants through immediate automated or manual notifications. Sentinel is committed to providing a continuum of case management operations to WSCA participating agencies that would allow for Sentinel staff to be located on-site for program operation. In addition to the standard requirements of this RFP, Sentinel is also proposing a completely offender funded program

		that would allow participating agencies to avoid collecting fees directly from program participants. Sentinel's case management model would allow for a full time office to be opened and local staff to be hired and trained. Once established this location could be utilized by participating agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand your programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates. Case supervision services are an integral component of the judicial process; therefore selecting the correct service provider is a critical decision. **Sentinel currently provides case management services to more than 100 programs from more than 50 locally-based offices across the country.** In these programs, Sentinel's staff monitors compliance to the court-ordered conditions with court orders via regularly scheduled meetings with each participant, addresses all issues of non-compliance, and reports continued non-compliance to the supervising agencies for resolution. Sentinel maintains individual case files on all participants for review by the court or its designees and in order to provide documentation for use in enforcement or revocation matters. Additionally, Sentinel has extensive experience customizing programs at the local level and currently **works directly with over 95 judges**. Through these programs, Sentinel's supervision services staff conducts more than **55,000 face-to-face defendant contacts a month**. Additionally, Sentinel understands the importance of expert court testimony and on a daily basis Sentinel has as many as **50 employees a day working in court rooms** nationwide testifying regarding participant activity. **This level of experience is difficult to replicate by any vendor and Sentinel is confident that its proposed program can exceed the court's expectations.** Sentinel has extensive experience provide the following staff members to programs utilizing its limited- or full-service case management services: **Program Director:** Dependent on the size of the specific program, Sentinel may employ a Program Director as the lead contact for the daily operation of the program and handle any court requests. The candidate will hold at minimum a Bachelor's Degree in social work or counseling and have counseling or social work experience with participants. This person's duties will include:

- Daily reconciliation of all payments received
- Supervision of all Sentinel office staff
- Quality assurance audits and reviews of supervision methodologies
- Oversee all contacts with victims
- Investigate all participants grievances
- Daily liaison for court personnel
- Court representative for any proceedings for participants
- Steering committee representative for Sentinel with court/agency personnel

Case Manager(s): Case Manager candidates will also hold at minimum of a Bachelor's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include:

- Adhering to Sentinel's Case Management Model including performing (1) Assessment, (2) Interpretation, (3) Case Planning, (4) Ensuring the Delivery of Services and (5) Evaluating Performance
- Explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature
- Create and maintain files on all participants referred to the program
- Process all payments
- Communication with court personnel if there are any inquiries on a specific participants
- Perform notifications of program completions/non-compliance

Administrative Assistant: Depending on the size of the specific programs and the volume of tasks placed on an office providing this type of service to a participant population, an Administrative Assistant maybe needed. This person will:

- Handle all calls received at the office
- Provide assistance to the Program Director and Case Manager(s) as needed
- Assist with performing any required transmission of reports
- General office tasks

IMPORTANT SENTINEL ADVANTAGE: Sentinel has helped pioneer the concept of opening local, community-based "Success Centers" where

		probationers/defendants/parolees can participate in electronic monitoring programs and optionally receive assistance with job placement, address drug addiction, as well as participate in cognitive skills classes, anger management and other developmental programs. Using this model, Sentinel can work directly with the participating agency and the courts to develop additional programs at its Success Center to help reduce recidivism **AT NO COST TO THE AGENCY**. Sentinel's basic business model rests on proven research that has shown that heavier punishment and long terms of incarceration or probation are not lasting answers to stem criminal behavior. Rehabilitation-oriented programs and defendant accountability, combined with community-based intervention and support, is the more sensible way to tackle this complex issue. Should participating agencies elect to utilize the Success Center Model, Sentinel will additionally provide the following staff members: **Program Specialist(s):** Program Specialist candidates will hold at minimum a Master's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include: ▪ Delivery of daily classes based on Diversion Orders or needs assessments ▪ Communication with the Project Director/Case Manager(s) regarding each defendants progress regarding his or her Case Plan ▪ Maintaining current on all applicable laws and changing regulations for class delivery
10b.11	a. Contractor will coordinate offender (in person) reporting on a schedule agreed upon by both parties	**Sentinel meets this requirement.** Sentinel Program Directors/Case Managers will be responsible for explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature. During Intake and Orientation, Sentinel will coordinate an agreed upon in-person reporting schedule with the participant based on the participants risk level assigned by the court and/or determined through Sentinel's risk assessment tools. Sentinel is capable and willing to provide monthly, bi-monthly, weekly and/or bi-weekly face-to-face offender compliance meetings in

		addition to daily monitoring of compliance or violation and the reporting of all participant activities. Please note that Sentinel understands that one of the main segments of an active case management program is the ability to verify that the offenders are abiding by all program regulations. Sentinel's program model is designed so that its program directors/case managers meet regularly with the program participants to review all of their activities and their activity documentation. **Sentinel has been successfully providing this exact program model to Los Angeles County since the early 1990's.**
10b.12	b. The contractor will confirm the employment status of the offender and financial status.	**Sentinel exceeds this requirement.** Sentinel will verify and confirm the validity of all pre-approved locations including work, school, college, counseling, AA/NA, victim awareness or other program classes and capture teacher/supervisor information for additional follow-up. **When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services.** Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors: (1) Present financial position. (2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position. (3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program. (4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision. **IMPORTANT SENTINEL ADVANTAGE:** During the course of any participant's monitoring, Sentinel will continue to confirm the on-going employment status of the participant and/or any changes financial status either during scheduled meetings or random spot checks/call to the place of employment.

10b.13	c. The contractor will collect fees from the offender and will provide notices to the government agency on delinquent payments	**Sentinel exceeds this requirement. Sentinel will be responsible for invoicing and the collection of fees from all participants.** Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of pending and/or over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc. Additionally, Sentinel local staff will promptly follow-up on missed or partial payments. Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason. **Additionally, should any participant become delinquent on payments, Sentinel will provide a delinquency notice to both the participant and participating agency informing them of the delinquency, detailing Sentinel's efforts for collecting fees from delinquent participants and Sentinel's recommended course of action regarding the participants continued monitoring.** Sentinel will also provide regularly scheduled (i.e. monthly, quarterly, etc.) reports to the participating agency and/or courts that provide details on all fees collected/uncollected from the offender-funded program. Sentinel **has monitored more than 1 million offender-paid electronic monitoring participants**. **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has directly collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies

		or victims at no additional charge to its customers.
10b.14	d. The contractor will review offender curfew activity from the time since the offender last reported.	**Sentinel meets this requirement.** During each scheduled compliance review, each participant will provide activity documentation to verify their whereabouts in the community since their previous compliance appointment. Sentinel's project director/case managers will also carefully review the daily alcohol monitoring reports as well as any curfew reports and/or GPS tracking maps that are available to verify that the offenders actually attended the activities they are permitted to by the participating agency and/or courts.
10b.15	e. The contractor will review monitoring /tracking activity with the offender and provide the government agency with exception reports for program violations.	**Sentinel meets this requirement.** During each scheduled compliance review, each participant will provide activity documentation to verify their whereabouts in the community since their previous compliance appointment. Sentinel's project director/case managers will also carefully review the daily alcohol monitoring reports as well as any curfew reports and/or GPS tracking maps that are available to verify that the offenders actually attended the activities they are permitted to by the participating agency and/or courts. Any violations, inconsistencies or incorrect documentation will result in a Non Compliance Report being issued to the participant and provided to the participating agency for review/enforcement.
10b.16	f. The contractor's case management activities shall be documented in the contractor's caseload management software and accessible to the government entity 24/7.	**Sentinel exceeds this requirement.** Sentinel designed its proprietary, web accessible case management software, SenTrack, specifically for use in the offender services arena. Employing SenTrack allows **real-time, on-line web accessibility** to participant case information and reports for Sentinel employees **and** authorized participant agency and/or court personnel. As the SenTrack case management software is an in-house concept and design, SenTrack is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support and recommends all participating stakeholders have access to the SenTrack software for program review and oversight.** **IMPORTANT SENTINEL ADVANTAGE:** SenTrack allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software. Sentinel catapulted the speed, capacity and capabilities of case management software through the development of the SenTrack SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective. **This translates into the ability to modify or**

develop new software variations as may be needed for the agency directly, in house, without having to utilize outside vendors which may bring data security concerns to the agency. Only Sentinel personnel would have access to the confidential participant data and the development of any new application.

Sentinel's SenTrack case management software incorporates all of the technology offered by Sentinel. The software is fully integrated in every Sentinel branch office and has become the foundation from which Sentinel serves its customers. Highlights of the SenTrack case management software include:

- Internet accessibility; available 24 hours a day to any Sentinel customer
- All client obligations to the court are tracked (courses, fines, drug screens, community service, restitution, demographics etc.)
- Real-time communication with Kiosks
- On-line payment acceptance
- Proprietary Case Management Software; 100% in-house support and customization available
- Over 150 available reports
- Customized reports provided at **no cost**
- Currently services more than 200 agencies and over 45,000 offender-paid participants
- Able to capture photo images as required
- Fully redundant and supported by continuous operation monitoring center designed to Underwriters Laboratory specifications
- Internal audit tools track all changes
- Unlimited query capabilities for detailed statistical reporting

The SenTrack system is completely customizable and currently provides more than 150 different types of case management and financial reports. Through the ability to customize the system, SenTrack has made it possible for judges to have the reports they want in the format they desire.

IMPORTANT SENTINEL ADVANTAGE: Due to Sentinel's extensive experience in providing case management and supervision programs, Sentinel has created and utilized its proprietary database system to manage all caseloads including compliance to the program's regulations. Along with status reports that Sentinel can provide to update the participant's program status to the

participating agency and/or court staff, Sentinel will also create non-compliance reports (NCR). Sentinel's non-compliance reports have easy "check-off boxes" that identify specific instances of non-compliance. The advanced Sentinel SenTrack system also allows for an on-going tally system showing the number of NCR's issued, along with the information as to how many remain "open" and how many have been resolved. This supplementary information is essential to agency staff trying to make a decision as to the participant's overall program compliance.

CONFIDENTIAL

Non-Compliance Report Screen in SenTrack: In the event that a participant does not comply with the regulations and conditions of the program, Sentinel staff will generate a non-compliance report that will include a narrative explaining the details of the situation, along with a quick-reference "check-off" box choice as illustrated

SPECIFICATIONS

These specifications are the minimum. The vendor has listed, clearly demonstrated, and presented features that add value, savings and/or reliability.

Although not currently required by the following specifications, it is intended that equipment available through this contract will meet or exceed the most recent version of the standard for offender tracking systems (OTSs) published by the U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. A draft standard was recently published for public comment dated June 2012. It was titled: **Criminal Justice Offender Tracking System Standard - NIJ Standard-1004.00.**

The following was excerpted from the NIJ Draft. - Two configurations of Offender Tracking System (OTS) models: one-piece configuration and multi-piece configuration. "In the one-piece configuration, the body-attached device contains the location methodology apparatus, communication device, battery, attaching straps and clips, indicators to the participant, and the casing. In the multi-piece configuration, there are two separate units. One unit is body-attached, and the other unit is body-worn. The components of the body-worn unit typically include the location methodology apparatus, communication device, battery, indicators to participant, and the casing. The components of the body-attached device typically include the transmitter/receiver, battery, attaching straps and clips, and the casing."

Definitions: "Body-attached: The quality of being physically secured to a participant's body." "Body-worn: The quality of being fastened, typically, to an article of the participant's clothing."

CATEGORY 3 – SATELLITE MONITORING AND REMOTE TRACKING SERVICE (GLOBAL POSITIONING SYSTEM (GPS)			
Responses below apply to <u>both</u> one-piece body-attached device and multi-piece tracking system.			
1.0	**SECTION A General Experience Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
1.1	General Experience	The Vendor shall have been in business for a minimum of three (3) consecutive years prior to proposal submittal.	**Sentinel exceeds this requirement. Sentinel has been providing electronic monitoring and participant supervision including electronic monitoring services for more than 20 years since its founding in 1992.** Sentinel is still currently in the business of providing electronic monitoring services to community corrections and/or criminal justice organizations and since its inception has had more than 1,000,000 participants successfully completed their programs through Sentinel's extensive continuum of community-based monitoring services. **Sentinel is proposing its latest generation, most advanced GPS tracking solutions, which has been in use for more than four (4) years in agencies nationwide. All of Sentinel's services, products and technologies are specifically designed for corrections supervision and will meet or exceed**

			the requirements for the Electronic Monitoring of Offender through the Western States Contracting Alliance. Please see the Bidder's Company Experience and History section of this proposal for more detailed information on Sentinel's experience with the provision of GPS tracking services.
1.2	General Experience	The proposed device(s) must have been in use and installed on offenders through one or more contracts with County, State, or Federal Government agencies. This experience must have been within the past 12 consecutive months prior to the proposal submittal date. Anytime Beta testing does not count toward the required experience.–The vendor's experience shall have been met with the vendor acting as the prime contractor in supplying the GPS device. Include these agencies in the response to Item 1.3 below.	**Sentinel exceeds this requirement.** Sentinel is proposing solutions for both one-piece and multi-piece configurations of GPS that include the latest generation, most advanced OM series one-piece GPS (from Omnilink Systems, Inc. – see enclosed letter from this manufacturer's executives pledging their support to Sentinel for this WSCA contract) and Sentinel's own TrakMate II Multi-Piece GPS tracking solutions, which have been in continuous use for more than four (4) years in government agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both these GPS tracking equipment in the Appendix D: Bidder Information and Profile section of this proposal as required. **Sentinel has been providing electronic monitoring and participant supervision services for more than 20 years since its founding in 1992.** Sentinel is still currently in the business of providing electronic monitoring services to community corrections and/or criminal justice organizations and since its inception has had more than 1,000,000 participants successfully completed their programs through Sentinel's extensive continuum of community-based monitoring services.
1.3	General Experience	The proposed device(s) must have been installed and in use on at least an aggregate of 500 offenders through one or more contracts with County, State or Federal Governmental agencies. This experience must include at least six (6) months of active monitoring for the model offered in response to this RFP. The vendor's experience shall have been met with the vendor acting as the prime contractor in providing all of the above services. Identify these agencies, volumes and devices in your proposal	**Sentinel exceeds this requirement.** Sentinel is proposing solutions for both one-piece and multi-piece configurations of GPS that include the latest generation, most advanced OM series one-piece GPS (from Omnilink Systems, Inc.) and Sentinel's own TrakMate II Multi-Piece GPS tracking solutions, which have both been in continuous use for more than four (4) years in government agencies nationwide and have each been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for both these GPS tracking systems in the Appendix D: Bidder Information and Profile section of this proposal as required.

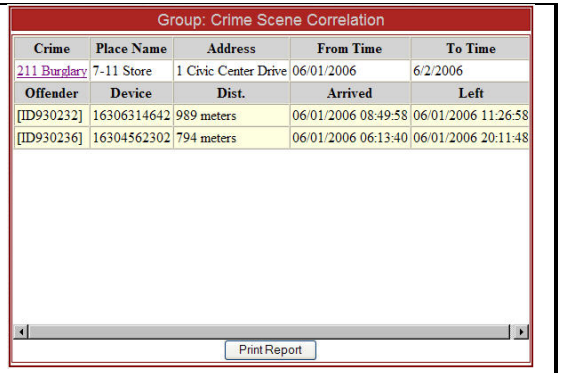
		response.	
1.4	General Experience	The proposed software must include the ability to compare the offender track points to crime locations from law enforcement Record Management Systems. This functionality must have been in use within the past 12 consecutive months, prior to proposal submittal date. This experience shall be with the same Government agencies listed in Item 1.3 above. 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.	**Sentinel exceeds this requirement. Sentinel was the first to develop and is the most experienced company providing Internet information exchange for monitoring and tracking information. SenTrak, Sentinel' advanced Internet information exchange platform, functions with Sentinel's the proposed GPS tracking equipment and has been in use consecutively for more than four (4) years in support of government agencies** with Sentinel acting as the prime contractor for equipment and services. The SenTrak software includes multiple capabilities to Proximity Report utility to perform date/time/location queries to compare if GPS participant(s) were in proximity of a particular address or location of a crime, including but not limited to Proximity Report and Event Detection. **IMPORTANT SENTINEL ADVANTAGE: Sentinel provides a Proximity Report utility capability that as has been in use for more than four (4) years in support of government agencies with Sentinel acting as the prime contractor for equipment and services.** This Sentinel report query is included at n additional cost and offers significant savings over other vendors such as who charge significant cost for their crime correlation software. This Sentinel solution can perform date/time/location queries to compare if a target GPS participant or multiple participants were in proximity of a particular address or location of a crime. The Proximity Report utility shows if a target offender or offenders were in proximity of a particular address or location of a crime. This report query can be generated by simply entering an address of interest including a crime incident report address, entering a date and time range, and executing the report query. These reports will stay within the system until a new address is entered but saved indefinitely for a permanent record through exporting the report to Excel. The Proximity Report shows the name of the offender, the date and time, Latitude, Longitude, distance to the address, the specific address identified, the offender device ID as well as an active link to view the tracking points via mapping for each participant identified by the query. The following is a sample report that can be exported into an Excel format.

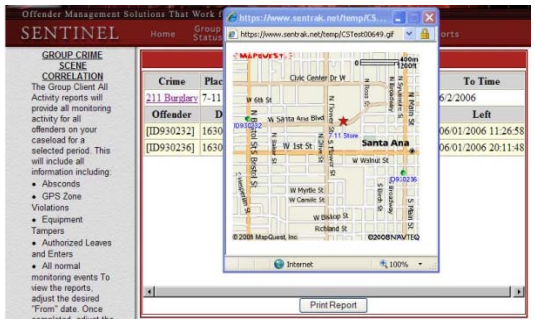
Name	Time	Latitude	Longitude	Distance (Feet)	Address	Device ID
W, Steve	2007-4-6 2:48 PM	34.09354322	-84.24284045	180	780 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-6 2:15 PM	34.09352468	-84.24284748	183	757 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-6 8:52 AM	34.09342423	-84.24279012	179	754 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-5 7:26 PM	34.09354933	-84.24286738	187	750 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-5 9:39 AM	34.09358673	-84.24274927	150	926 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-5 9:36 AM	34.09357278	-84.24273554	147	933 Windward Pkwy, Alpharetta, GA, 30005	6782061310
W, Steve	2007-4-5 8:32 AM	34.09367501	-84.2428532	181	862 Windward Pkwy, Alpharetta, GA, 30005	6782061310

Sentinel's "Event Detection" feature is a built-in feature of the SenTrak web-based monitoring application that is currently being offered to WSCA. Most vendors who offer crime correlation software require users to access a separate program, which increases the time and effort necessary to reach the desired data. By incorporating the "Event Detection" or location correlation into the main application portal, Sentinel is able to offer itscustomers the ability to initiate a query against the entire population of offenders on GPS tracking in just a matter of minutes in four easy steps and on-demand, to determine precise information regarding an offender's location. Officers can enter the date, time and location of any crime and promptly receive a report of all offenders who were near the scene. The results of the query can also be displayed graphically on an individual map, which allows the event and plotted offender information, relative to the query, to be viewed.

The "Event Detection" feature is accessed under the Reports menu in SenTrak. Once accessed, the officer will then input location information, including street address, city, state and zip code. Next the officer will enter the type of crime along with the date and time of the incident. A specific radius is then input in order to generate a report of all offenders who were near the specified location of the crime. Officers are able to perform these searches 24 hours per day, seven (7) days per week, 365 days

			per year from any Internet–enabled computer with proper access rights to the SenTrak software. Upon completion of the entry of the event information, a report of all offenders within the specified radius is displayed in a table. This report displays the offender's identification number, the device number, the distance from the crime scene, and the time of entry and departure from the area. By placing the mouse over the offender's ID, the offender's name and address can be displayed in a pop-up window. This report can be viewed on screen or printed for later review. In order to allow cross-jurisdictional queries without creating unauthorized information release, agency's and supervising officer's information are not provided. Sentinel can make this data available upon notification to the supervising agency and officer of the relational "hit". Once authorization is received, Sentinel can place the two (2) agencies in communication with one another in order to determine the relevance of the data. Once the table is generated, a map can then be displayed by clicking on the Crime Type. This map distinguishes the crime location by placing a red star upon the location. Each offender within the specified radius of the crime is noted by a green dot along with the client's identification number. Sentinel will provide location correlation capability to each WSCA participating agency throughout "Event Detection" reports at no additional cost.
1.5	General Experience	The Vendor shall provide a secure confidential monitoring service center and help-desk facility. The Monitoring Center	**Sentinel exceeds this requirement. IMPORTANT SENTINEL ADVANTAGE: Continuity of Monitoring Services:** All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine,





		Facility and Services must have been in use for at least 12 consecutive months through one or more contracts with County, State or Federal Governmental agencies at the time of proposal submittal. This experience shall be with the same government agencies listed in Item 1.3. The Vendor shall have been the prime contractor for any contract services performed by any subcontracted monitoring service center or help-desk facility.	California and Atlanta, Georgia) delivering **all monitoring services and help desk operations from one centralized source – Sentinel**! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring operate their GPS monitoring center and help desk however, they admitting to outsourcing monitoring services/help desk services to third-party providers for both radio frequency and alcohol monitoring thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.) **The Sentinel secure confidential monitoring center and help desk have been servicing WSCA participating agencies as a prime contractor since January 2, 2002 (over 11 years). Sentinel understands the objectives of the Western States Contracting Alliance program better than any other vendor in the industry.** **The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis.** The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted, monitoring information is disseminated and technical support (help desk) services are provided to all Sentinel customers including those listed in Item 1.3. Sentinel operates both its primary monitoring center located in California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. To maintain monitoring center operational integrity and confidentially, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside

			security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** All monitoring services will be provided by Sentinel. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** The Western States Contracting Alliance participating agencies can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year. Sentinel strives to resolve any customer inquiries promptly and on the first

			contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert, and changing a participant's schedule. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Regional Account Manager/Field Operations Manager for customer enhancement requests, suggestions and ideas.
1.6	General Experience	The Manufacturer shall have an ISO 9001 certification.	**Sentinel exceeds this requirement.** Much of Sentinel's success hinges on Sentinel's top management's commitment to continual process improvements, which is a main goal of the ISO 9001:2008 Quality Standard. **Sentinel's manufacturing division received ISO 9001-2008 accreditation in January 2009 and the manufacturer of the OM series GPS received certification in 2006.** Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments and to ensure all staff has access to needed resources and training to support the quality management system. Sentinel has provided copies of the certifications in the Exhibits section of this proposal.

1.7	General Experience	The device and accessory items shall be currently registered and approved by the Federal Communications Commission (FCC).	**Sentinel meets this requirement.** All of the proposed equipment complies with all appropriate FCC regulations. Sentinel has provided the Identifier Numbers below and copies of the certifications are included in the Exhibits section of this proposal: **Part 15** ▪ OM210 TS5-6050M-OM200 ▪ TrakMate II Transmitter OEHDUALTRAKPID ▪ TrakMate II Tracking Device QFPTGP79AE
2.0	**SECTION B Monitoring Center Facility and Monitoring Center Interactive Services**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
2.1	Facility	Deleted.	
2.2	Facility	The Vendor's monitoring center shall have a permanently installed and functioning emergency backup power source, independent of its main power source, capable of maintaining continuous operations, for a minimum of forty-eight (48) hours, in the event of failures of normal utility power. If power is not restored, a back-up monitoring center service is activated within 60 minutes.	**Sentinel exceeds this requirement. Sentinel's monitoring centers have permanently installed and functioning emergency backup power sources, independent of its main power source, capable of maintaining continuous operation until primary power is restored or the backup monitoring center is fully functional.** Sentinel understands the importance of having reliable primary and supplementary power resources available at all times. With its monitoring centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. To assure that all services are continuously maintained in the event of a major disruption, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-the-art technology including: ▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator. Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and

			can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's on-site diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled. The diesel generator is regularly inspected to ensure that it remains in operational order at all times. **Through the use of Sentinel's on-site UPS unit and diesel generator, Sentinel's monitoring center can operate through any loss of commercial power, even over an extended period of days (in excess of 72 hours). Sentinel has never lost any data or performance capability due to power losses of any sort.**
2.3	Facility	The Vendor's Monitoring Center shall have ventilation and temperature controls adequate to ensure proper functions of the monitoring center hardware.	**Sentinel meets this requirement.** The continuously staffed Sentinel monitoring center resides in independently secured, climate-controlled, properly ventilated facilities with raised floors to ensure proper functions of the monitoring center hardware and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community.
2.4	Facility	The Vendor's Monitoring Center's physical security features at a minimum shall include closed circuit camera system and limited access doorways. Describe other features to ensure physical security.	**Sentinel exceeds this requirement.** To maintain monitoring center operational integrity, and physical security, Sentinel's monitoring center's physical security features include closed circuit camera system and limited access doorways. Additionally, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring

			center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building. The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified.
2.5	Facility	The Vendor shall have a secondary (backup) Monitoring Center capable of providing full operational functions in the event the primary monitoring center is	**Sentinel exceeds this requirement.** Sentinel has a redundant monitoring center located sufficiently distant from the primary center, that 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. To

		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.	support business operations for electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a fully-redundant monitoring center. Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart so it will be unaffected by a manmade or natural event or loss of electrical or communications services that would disable the primary monitoring center. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, Sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.6	Facility	The Vendor shall 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.	**Sentinel exceeds this requirement.** The Sentinel monitoring center features the following technology for its redundant Internet and telephone communications: ▪ T-1 telephone trunks, provided from three (3) redundant leading providers, to prevent against outages ▪ 432 Fiber-optic telecom cable lines and 200 POTS lines fed directly into the Sentinel facility ▪ Primary provider, Cox Communications (a leading provider of

			communications) is regionally headquartered within 8 miles and has triple electrical and data redundancy ▪ Second redundant carrier, AT&T ▪ Third redundant carrier, TW Telecom ▪ Cisco IP Telephony Solution combined with Cisco Networking for providing statistical tracking of all data and telephone activity A confidential, predefined and rehearsed protocol is set up with Sentinel's telecoms provider to enable a rapid transfer in accordance with the agreed service level. The back-up call handler functions in an active state and is ready to receive calls from the monitoring units as soon as the calls are rerouted from the primary call handler by Sentinel's Telecom providers. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart so it will be unaffected by a manmade or natural event or loss of electrical or communications services that would disable the primary monitoring center. Sentinel's secondary redundant electronic monitoring center is fully operational and staffed during normal business hours is capable of being promptly staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.7	Facility	The Vendor shall perform complete support of all interface hardware and software equipment (within the monitoring center) necessary to ensure provision of the service for the duration of the contract.	**Sentinel exceeds this requirement.** Support of all interface hardware and software equipment will be provided by Sentinel personnel and equipment through its state-of-the-art monitoring facility located in Irvine California that houses the central computer system and monitoring personnel responsible for supporting the proposed solution. **Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations for the duration of the contract.** **IMPORTANT SENTINEL ADVANTAGE:** To support operations for database replication of key IT, and failover disaster recovery to avoid unnecessarily excessive downtime due to hardware or software issues,

			Sentinel's monitoring system incorporates 100% redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers are located in Atlanta, Georgia, over 500 miles apart. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. Redundant web servers, application servers and database servers are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred.
2.8	Facility	The Vendor shall provide the Agency a contact number, accessible twenty (24) hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced.	**Sentinel meets this requirement.** Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center. All monitoring services including receipt of problem reports and problem resolution will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Additionally, Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.**
2.9	Facility	In the event any component of the Vendor's monitoring center service becomes inoperable, the Vendor shall immediately notify the Agency Program	**Sentinel meets this requirement.** In the event any component of Sentinel's monitoring center service becomes inoperable, Sentinel will notify all affected participating agency Program Managers or designees by telephone, no later than 30 minutes after service failure.

		Manager or designee by telephone, but no later than thirty (30) minutes after service failure.	
2.10	Services	The Vendor's back up Monitoring Center must be activated within 60 minutes of initial system failure or disaster.	**Sentinel meets this requirement.** Sentinel operates two (2) geographically redundant monitoring centers in Irvine, California and Atlanta, Georgia. To support business operations for electrical power loss, telephone equipment failure and failover disaster recovery, Sentinel's monitoring system incorporates a fully-redundant monitoring center. Sentinel's primary monitoring center is located in California with a back-up monitoring center in Atlanta, Georgia over 500 miles apart. **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly **(within 60 minutes)** staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business.
2.11	Services	The Vendor's primary Monitoring Center shall be fully operational and staffed adequately to support the operations of this Contract, twenty four (24) hours a day, 365 days per year, with highly skilled technicians that have completed a	**Sentinel exceeds this requirement.** Sentinel **operates** both its primary monitoring center located in Irvine, California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with highly trained technicians and personnel, from which Sentinel

		minimum of 40 hours initial training and ongoing annual training. Staffing levels must meet the device ratio for the Agency activated equipment.	handles over 50,000 calls on a daily basis. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **As such, staffed monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year.** **IMPORTANT SENTINEL ADVANATGE:** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a monitoring center failure or service catastrophe and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbent WSCA Alcohol Monitoring electronic monitoring contractor for more than 11 years since the WSCA contract's inception.** **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's monitoring center is staffed with bilingual personnel on every shift in order to ensure successful interactions with its agency customers. Sentinel monitoring center personnel typically answer 96% of all calls within eight (8) seconds and provide an on-hold wait time of four (4) seconds or less. All of Sentinel's monitoring center employees undergo a thorough and detailed training and certification program, during which they are trained in all aspects of electronic monitoring equipment and software including troubleshooting and the necessary alarm procedures to ensure timely and accurate notifications. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel monitoring center staff is cross-trained to support assistance requests for radio frequency (RF) electronic monitoring, voice verification monitoring programs, breath alcohol testing (BAT), transdermal alcohol monitoring and **global positioning satellite (GPS) tracking** should any participating agency be utilizing more than one (1) service category. Two (2) full weeks are used during the training of a new monitoring center operator to ensure that a thorough electronic monitoring knowledge based is

			developed. Complete equipment functionality and software platform protocols must be understood prior to graduation to a Level One Monitoring Center Operator. The training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge- and performance-based, allowing maximum participation by monitoring center staff and supervisors. The training techniques, tools, and exams are developed by the training coordinator and are required to successfully complete the certification process. The coordinator will conduct training sessions at regularly scheduled intervals; however, each shift supervisor will be instrumental in the development of their employees. **Monitoring Center On-going Training:** To maintain an efficient service oriented organization, Sentinel employs on-going training modules for all positions. This method is applied equally to all monitoring center operators as to allow correct interpretation and dissemination of information to all authorized agency personnel. The training modules for each employee within the monitoring center are delineated. Sentinel is committed to providing the highest level of monitoring services in the industry. A critical element of providing reliable and efficient monitoring is a knowledgeable, professional and well-trained staff. This training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge and performance based, allowing maximum participation by monitoring center staff and supervisors. A grading system has been established to easily identify staff members with certain knowledge and ability. This grading system requires an employee to demonstrate acquired skills through verbal and written examinations. **Levels:** ▪ Monitoring Specialist Level – Trainee ▪ Monitoring Specialist Level – 1 ▪ Monitoring Specialist Level – 2 ▪ Monitoring Specialist Level – 3 ▪ Monitoring Shift Supervisor

Training / Certification: The Training Coordinator is responsible for developing the training techniques, tools, and exams that are required to successfully complete the certification process. The Training Coordinator will conduct training sessions at regularly scheduled intervals; however each shift supervisor will be instrumental in the development of their employees. Training for the various levels will be conducted as follows:

Level	Training Conducted By	Certified By
Trainee	Training Coordinator	Training Coordinator
1	Shift Supervisor	Training Coordinator
2	Shift Supervisor	Training Coordinator
3	Training Coordinator	Training Coordinator
Shift Supervisor	Monitoring Center Manager	Monitoring Center Manager

Certification Exams: A written examination is prepared for each grade level. Some grade levels require that an employee demonstrate acquired skills. A minimum test score is required to pass the written examination.

Level	Minimum Score
Trainee	85%
1	85%
2	85%
3 / Shift Supervisor	90%

A passing score is mandatory for the Trainee and Level 1 position and is required for continued employment. The Level 1 certification exam must be successfully completed before the expiration of a new employee's orientation period. Re-testing periods are established to give an employee an additional attempt to achieve a passing score.

Level	Testing Period	Re-Testing Period	Passing Score
Trainee	When initial training complete	14 Days	Mandatory
1	10 weeks' employment	14 Days	Mandatory

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>2</td><td>90 Days</td><td>30 Days</td><td>Not Mandatory</td></tr>
<tr><td>3</td><td>90 Days</td><td>30 Days</td><td>Not Mandatory</td></tr>
</table>

A passing score is mandatory for continued employment beyond the orientation period for the Trainee and Level 1 grade.

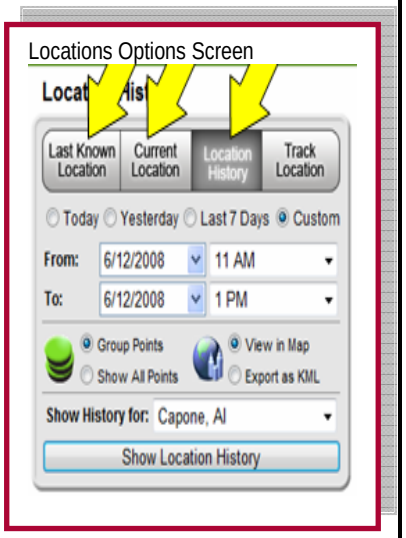
Promotion: This performance-based program ensures that qualified candidates are promoted in a manner consistent with Sentinel's goal of maintaining a knowledgeable and professional staff. A staff member will be promoted upon successful completion of the certification process. An employee that meets the length of service requirements for a grade promotion must be recommended for advancement by their supervisor. Supervisors are advised to consider the following items before recommending an employee for promotion.

Performance:
▪ Attendance
▪ Dependability

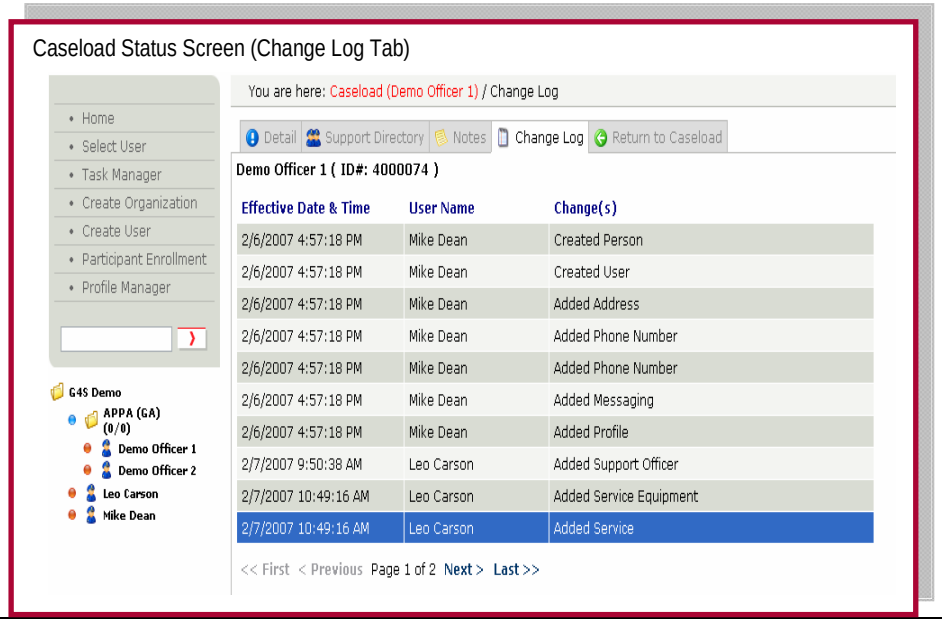
Measuring Tools:
▪ Report
▪ Charts
</td></tr>
<tr><td>2.12</td><td>Services</td><td>The Vendor must provide a staffed communication system utilizing an 800-telephone number an 800- number fax, and email access, available 24-hours per day, 365 days per year at no additional charge to the Agency for technical, analysis, and application assistance.</td><td>
Sentinel exceeds this requirement. Staffed customer service and technical support operators are available through a toll-free telephone number, toll-free facsimile numbers and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center for technical, analysis, and application assistance at no additional charge to the participating agencies. All monitoring services will be provided by Sentinel. Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.

IMPORTANT SENTINEL ADVANTAGE: Continuity of Monitoring Services: All proposed technologies are monitored from redundant, staffed monitoring centers (Irvine, California and Atlanta, Georgia) delivering all monitoring services and help desk operations from one centralized source – <u>Sentinel</u>! Simply put, this directly and significantly enhances continuity and productivity of officers/users. (In contrast, as admitted at the WSCA pre-proposal meeting, companies like 3M Electronic Monitoring operate their GPS monitoring center and help desk however, they admitting to outsourcing
</td></tr>
</table>

			monitoring services/help desk services to third-party providers for both radio frequency and alcohol monitoring thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.) **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are operational 24 hours a day.** Sentinel's secondary redundant electronic monitoring center in Atlanta, Georgia is fully operational and staffed during normal business hours is capable of being promptly **(within 60 minutes)** staffed 24 hours a day, seven (7) days a week in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.13	Services	The Vendor's Monitoring Center must be able to support interactive queries from authorized Officer's and/or authorized law enforcement agencies, (including an offender's location by date range and/or time range when requested), within 5 minutes.	**Sentinel exceeds this requirement.** Sentinel monitoring center operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies. Each monitoring center operator has the expertise to easily respond to interactive queries from authorized officer's and/or authorized law enforcement agencies, (including but not limited to identifying an offender's location by date range and/or time range when requested), within 5 minutes. Sentinel strives to resolve any customer inquiries promptly and on the first contact and the majority of technical problems are resolved through technical telephone support, through remote diagnostics, or through equipment replacement using the on-site spares. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, changing a participant's schedule, performing participant enrollments or entering data into the system. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported

			by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Account Management/Field Services personnel for customer enhancement requests, suggestions and ideas. **IMPORTANT SENTINEL ADVANTAGE:** Additionally, since the OM series devices are always active and communicate through cellular coverage, authorized users will have the ability to perform on-demand location verifications. In fact, the web-based software enables agencies to view Last Known Location and Location History as well as Current Location.  Real-time participant information, including on-demand location verifications, can be accessed through the software Location History window "Current Location" button as shown to the right. While this on-demand location information is accessed at the time of request, virtually instantaneously, Last Known Location gives the user the fastest information, taking the last point stored and displaying it on the map. The time of the point is given, along with the relative address and latitude and longitude. If more current information is needed, selecting Current Location will instruct the software to contact the device, perform an immediate location and display it on the map.
2.14	Services	The Vendor's Monitoring Center Service	**Sentinel exceeds this requirement.** Staffed customer service operators are

		must be able to provide for offender enrollments and scheduling to be performed via direct telephone request (password accessible) when Agency staff (officer) does not have immediate access to an internet connection.	available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies. **The Sentinel monitoring center is readily accessible toll free by phone (password accessible) process service requests when agency staff (officer) does not have immediate access to an internet connection.** Sentinel monitoring center operators have the expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, **entering or changing a participant's schedule, performing participant enrollments or entering data into the system**. Operators can also provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. **Each participating agency staff member will be supplied with a unique verbal password which must be provided to the monitoring center operators when calling in to request data modifications.**
2.15	Services	The Vendor's Monitoring Center Service should be able to enroll or deactivate GPS tracking services for an offender within 30 minutes after receipt of request by fax, telephone or e-mail notification from an the Officer.	**Sentinel exceeds this requirement.** Staffed customer service operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies. **Sentinel will process all requests to enroll or deactivate GPS tracking services for an offender within 30 minutes after receipt of request by fax, telephone or e-mail notification from an officer.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.**
2.16	Services	The Vendor's Monitoring Center Service must maintain accurate and concise historical logs of all telephone, text message, emails and fax calls attempted and completed, including date, time, and the associated incident. The Vendor shall make these logs available to the Agency upon request.	**Sentinel exceeds this requirement.** All telephone calls to and from the monitoring center are recorded for training and auditing purposes and are available for later playback. Additionally, the central computer system continuously receives and retains all monitoring data received, text messages, emails and fax calls attempted and completed, including date, time, and the associated incident**. The SenTrak system automatically logs all changes performed in SenTrak with the user's name, date and time of the change, and change the user made.** Sentinel tracks **all** changes to the application, including but not limited to participant or agency details, notes, alert notifications attempted or completed (text message, email, call or fax), alert resolutions, enrollments, terminations and service requests. **This information is viewable through the SenTrak Change Log and provides agencies with a**

			clear audit trail for user accountability. 
2.17	Services	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 Agency staff when an alert notification is generated. The Vendor's monitoring service shall include the capability to administer a phone call by a live staff person in the monitoring center in response to designated priority alert notifications, at an additional fee.	**Sentinel meets this requirement.** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately 24 hours a day, seven (7) days a week to designated participating agency staff. Sentinel supports all standard methods of notification, such page (alpha or numeric), electronic mail, fax, and/or text message to a cell phone. In addition to automated notifications, Sentinel offers triage services via monitoring center staff whereby live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage for up to three (3) alert notifications, (i.e. bracelet strap, low battery, zone violations) before the system

			generates notification should the agency request this service and additional alerts will be priced on an optional price plan..
2.18	Services	The Vendor's Monitoring Center service must triage alerts, including triaging and responding to alerts with direct contact to both Agency staff and offenders for resolution as defined by the Agency. The Monitoring Center service must have the ability to escalate an alert notification if the officer does not acknowledge the notification within an Agency-specified time to the next Agency designated contact. In the event an alert notification is unresolved, the Vendor's Monitoring Center service shall be responsible for contacting the Agency's designated officer via, text message, fax, email or phone. The means or mode of contact shall be at the Agency's discretion. These services shall be provided twenty-four (24) hours 7 days a week. The Vendor's Monitoring Center Alerts will be triaged and responded to for up to three (3) alert notifications, (i.e. bracelet strap, low battery, zone violations), additional alerts will be priced on an optional price plan.	**Sentinel exceeds this requirement.** In addition to automated notifications, Sentinel offers triage services via monitoring center staff 24 hours a day, seven (7) days a week whereby live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to manual triage for up to three (3) alert notifications, (i.e. bracelet strap, low battery, zone violations) before the system generates notification should the agency request this service and additional alerts will be priced on an optional price plan.. Sentinel will be responsible for maintaining a call tree that will be utilized when contacting participating staff to report alarm notifications pursuant to established protocols. Sentinel understands that if an acknowledgment by one of the participating agency staff members is not made or received within a specified time frame, the alarm notification shall be automatically returned to the monitoring center system, and the call tree escalation process shall be implemented. **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel provides an automated system through toll-free 800 number for officers to call in and acknowledge receipt of an alert through the AMS system. Through this system, Sentinel is able to receive a verifiable confirmation via a telephone call or text message response to the monitoring center to confirm that all immediate alarm notifications were received and/or acknowledged by Western States Contracting

			Alliance participating agency staff. **IMPORTANT SENTINEL ADVANTAGE:** Unlike other vendors, Sentinel's proposed solution allows for automated acknowledgement AND automated escalation procedures. As this is completed through the software, this eliminates the possibility for human error therefore creating a more accurate and reliable system of escalation.
2.19	Services	The Vendor's Monitoring Center Service must provide the capability for every human voice call in and out of the system to be recorded with a transaction record that indicates the called number or calling number, and the result of the call. This information shall be made available to the Agency Program Manager at the Agency's request.	**Sentinel exceeds this requirement.** All telephone calls to and from the monitoring center are recorded for training and auditing purposes **and are available for later playback**. Sentinel tracks **all** transaction records indicating the called number or calling number, and the result of the call. Sentinel will make this information available to the respective participating agency Program Manager upon request.
2.20	Services	The Vendor's Monitoring Center must provide an initial response to pre-determined alert notifications to troubleshoot and resolve the notifications per established protocols as agreed to by both the Agency and the Vendor and optional price plan.	**Sentinel exceeds this requirement.** Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. At no additional cost, Sentinel will customize each individual participating agency's notification profiles to perform initial troubleshooting and resolution of pre-determined notifications should the agency request this service. In addition to automated notifications, Sentinel offers triage services via monitoring center staff whereby live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts. Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating

			agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record.
2.21	Services	The Vendor's Monitoring Center service must be able to tailor the level of alert notification to the Agency or individual needs or protocols.	**Sentinel meets this requirement.** Sentinel's monitoring service can tailor the level of alert notification to meet individual agency needs and protocols, including but not limited to all aspects of notification defined by this WSCA RFP. Prior to each program deployment, Sentinel will meet with the participating agency staff to create a Notification Requirements matrix providing the protocols for each type of alert, notified officer, time of notifications, and preferred method of communication. Thereafter, Sentinel's Account Manager will maintain regular communication with county personnel and department staff to update and/or tailor the matrix to the needs of the agency and program. Sentinel Monitoring Services are ISO 9001:2008 certified and maintain **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations **including agency/departmental specific operational procedures for monitoring, notification protocols, technical support and/or customer service.** SenTrak provides many advanced features including the capability to determine notification protocol(s). Sentinel will work with the agency to determine and program appropriate agency notification profiles based on the type of program and level of risk to public safely of its participants. Each agency will have the capability to determine an agency specific level or levels of notification. Each authorized user within the agency will then have the ability to choose from the agency-determined notification protocols on a per participant basis. For example, an officer can choose to receive only an email notification of violations for a particular participant but may choose to receive a telephone call and an emailed report of the violation for a different participant. Additionally, individual users can choose to exclude certain events from notification if deemed unnecessary on a per participant basis. These events would still be included on daily, weekly or monthly reports. Notification methods can also vary by supervising personnel.
2.22	Services	The Vendor's Monitoring Center must be responsible to maintain a call tree to be utilized when contacting Agency staff to report alert notifications pursuant to	**Sentinel exceeds this requirement.** Sentinel will be responsible for maintaining a call tree that will be utilized when contacting participating agency staff to report alarm notifications pursuant to established protocols. Sentinel understands that if an acknowledgment by one of the participating agency staff

		established protocols and optional price plan.	members is not made or received within a specified time frame, the alarm notification shall be automatically returned to the monitoring center system, and the call tree escalation process shall be implemented. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel operates a highly unique automated system via toll-free 800 number for officers to call in and acknowledge receipt of an alert through the Automated Messaging System (AMS). The AMS enables officers secure use of touch tones to rapidly acknowledge receipt of an alert and stop ongoing escalation. The AMS also allows offices to immediately connect to a live monitoring center operator or, as always, officers who prefer to clear alerts via voice telephone call with a live operator may call Sentinel's monitoring center direct and toll free 24/7 to do so as an alternative to the AMS. Sentinel's AMS is complemented by web-based audit capabilities capable of tracking the performance of both Sentinel and the agency's staff/program regarding notification steps and response for each alert. Sentinel's software provides management information reports capable of querying the details related to alert response. Authorized users can perform web-based report queries on any alert(s) to determine: the number of notification steps taken, the contacts(s) and method(s) used to attempt notification and the individual who ultimately confirmed receipt of notification – each accompanied by the date/time of occurrence. This unique Sentinel capability provides unparalleled accountability for user agencies. **IMPORTANT SENTINEL ADVANTAGE:** Unlike other vendors, Sentinel's proposed solution allows for automated acknowledgement AND automated escalation procedures. As this is completed through the software, this eliminates the possibility for human error therefore creating a more accurate and reliable system of escalation. **IMPORTANT SENTINEL ADVANTAGE:** If an alarm notification is unresolved, the Sentinel monitoring center will contact the participating agency's designated officer via, text message, fax, email or phone as directed by participating agency's call tree and notification protocol. All comments entered as part of clearing alerts (regardless whether by officer or by monitoring staff) are attributed in the system as part of the alert record.
2.23	Services	In the event of an alert violation, the monitoring center service must provide to the Officer, at a minimum the Offender's name, type of violation, time of violation,	**Sentinel exceeds this requirement.** Alert notifications sent to department staff will include, at a minimum, the program participant's name, the nature / type of the alert, the date and time of the alert, and the Last Known Location and current battery level and follow-up actions as well as any actions (other info), if

		and the time and location of the Offender's last known location.	any, taken by Sentinel staff. **IMPORTANT SENTINEL ADVANTAGE:** Each alert provides a variety of information designed to assist officers to investigate or confirm a participant's violation status including but not limited to the purpose for the notification, participant's contact phone numbers, participant's physical description and last known location. Providing this information through the notification process proactively increases officer efficiency by eliminating the need for the officer to log into the system to obtain the necessary information to investigate alerts, allowing quicker case management response times.
3.0	**SECTION C Data Center, Data Storage, and Data Access**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
3.1	Data Center	The facility housing the Data Center(s) must have multiple physical security features. Describe the physical security features that protect the Data Center and agency data.	**Sentinel meets this requirement.** **Physical Security One-Piece GPS Data Centers:** The one-piece GPS data centers use state-of-the-art technology and best practices for securing both the facility and the data. This includes the following: ▪ Four (4) physical layers of security, including but not limited to access doors that are monitored and alarmed for tamper protection, all of the environmental control alarms are connected into the main security panel located at the security desk and the onsite Network Operations Center (NOC). ▪ State-of-the-art access card system ▪ Trained security personnel ▪ Closed circuit television cameras (CCTV) that record and monitor activity both inside and outside the facilities ▪ Biometric and Key Card secured facility ▪ 24 hours a day, seven (7) days a week on-site staffing from dedicated security and storage engineers **Physical Security Two-Piece GPS System:** The primary monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This monitoring center facility houses the data centers utilized to support the proposed two-piece GPS tracking solution. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and its data by upholding the following security

			standards: ▪ Enforces an electronic key card system for entryway access to both outside building and monitoring center ▪ Uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways ▪ Archives data daily and stores it in a secure location to protect against memory loss in case of power failure Additionally, the Irvine facility is equipped with a sophisticated security system designed to limit and control access while monitoring via Closed Circuit Television (CCTV) its immediate and surrounding areas. Sentinel's monitoring center and secure web-based monitoring systems (accessible only via secure username and password) incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its systems. For security purposes, the Irvine site does not conduct any business with the general public as it contains Sentinel's corporate office and monitoring center. Program participants or monitored defendants have no access to this facility. The primary monitoring center is located on the second story of Sentinel's Irvine facility thereby eliminating access through any ground floor level window. There are only two (2) access ways into the monitoring center and each one of these doorways remains electronically locked at all times. For access through these doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only monitoring center personnel who are on duty for their shift are allowed to enter the center. As added security, each of the two (2) access ways into the monitoring center are monitored via a closed circuit television system that is supervised from inside the Irvine facility. All monitoring center personnel have continual direct access to a 911 emergency line in the event that an intruder attempted to gain access into the monitoring center. For outdoor perimeter security, the property management firm that owns that property provides random security patrols for the building.

			The CCTV equipment is installed in and around the monitoring center. The cameras are monitored and recorded 24-hours per day and surveillance tapes are labelled and archived for a period of 60 days. Every entrance to the monitoring facility is under CCTV surveillance. In addition to Sentinel's CCTV and electronic access, an independent security provider monitors the monitoring center's alarm system. If the facility is compromised or the supervisor's panic button is depressed, the local authorities are immediately notified. **Security of Monitoring Records:** In Sentinel's experience with offender populations nationwide, Sentinel understands the importance of data integrity both in its actual data entry as well as its subsequent data retention. To ensure that the proper information is entered at all times, Sentinel's personnel are thoroughly trained on data entry procedures with supervisorial support for any adjustments or corrections. Each user is given their own login and once they set their confidential password Sentinel can ensure the integrity of each user's entry. This unique user access allows Sentinel's Information Technology personnel to follow electronic audit trails that allow supervisors and management to verify the source of all date entry. The workstations that Sentinel's staff and agency personnel use at the monitoring center and/or local facilities are technically only used to connect to Sentinel's central server systems. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. In addition, Sentinel's monitoring center, data centers and secure web-based monitoring system incorporates the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure

			the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Any instance of failure resulting in a loss of monitoring capability will be reported to the participating agency. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. All of Sentinel's security systems are monitored continuously. **Monitoring System Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. To prevent unauthorized access from outside the monitoring and/or center, the software uses leading Internet security features, including 128-bit encryption. The proposed monitoring platform uses Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Sentinel also employs multiple firewalls designed to keeps outside computer users from interfering with the internal network operations and to also keep them from retrieving private information from other network computer systems. Sentinel utilizes a firewall appliance that is regularly monitored and reviewed to be sure that the appliance is properly functioning and to monitor unauthorized activity.** The firmware (software) that is running on the appliance is regularly updated to ensure Sentinel has the latest security technology patches, fixes, and updates and that they are properly applied. The appliance monitors all Internet traffic that goes in and out of the monitoring servers, to and from its ultimate destination to ensure that the data / traffic is adhering to the set rules that are in place on the Internet Firewall appliance. All of the firewall and/or remote access dial-in connections will stop

			any messages they are not specifically told to allow. **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.2	Data Center	The Vendor's Data Centers must have ventilation and temperature control adequate to ensure proper functions of the Monitoring Center hardware.	**Sentinel meets this requirement.** The data center facilities used to house the data received from both the proposed one-piece and two-piece GPS tracking solution reside in independently secured, climate-controlled, properly ventilated facilities with raised floors and written policies and procedures for access that meet all applicable federal, state and local regulations and do not endanger the health and safety of employee or the community.
3.3	Data Center	The Vendor's Data Centers must have multiple redundant back-up generators.	**Sentinel meets this requirement.** Sentinel understands the importance of having reliable primary and supplementary power resources available at all times having multiple redundant back-up generators. With its data centers continuously online 24 hours a day, seven (7) days a week, Sentinel has taken all necessary precautions to ensure that its power access remains at 100% at all times and remains seamless to its customers and program participants. The one-piece GPS data center's electrical infrastructure consists of two major components:

			▪ A redundant primary distribution system ▪ An emergency power generation system APS provides the distribution system with dedicated power sources. The system is based on a redundant diverse distributed system consisting of the following: ▪ Uninterruptible Power Supplies (UPS) ▪ Demarcation Power ▪ Power Distribution Units (PDU) ▪ Utility Service Bus (USB) All computers, routers, phone systems, alarm systems and related power systems have Uninterrupted Power Supplies (UPS) capable of extended battery backup. In case of power failure, the UPS will automatically maintain power to all key computers, lighting, security, network, communications and related systems. An audible alert informs staff that the UPS systems are engaged. Additionally, there are **two (2) independent utility power feeds on different sub-stations. The emergency power generation system consists of Automatic Transfer Switches (ATS), Emergency Service Bus (ESB) and redundant diesel generation. In the event of a power failure of both of the two (2) independent utility power feeds, the emergency diesel generators will provide power in less than 10 seconds, and contain 1,000 hours of fuel for superior back-up performance.** Once started, the generator automatically ensures it is operating at sufficient capacity and then switches power from the grid to the generator. Data center staff will conduct regular hourly inspections of the generator to ensure the maintenance of adequate fuel and proper operating parameters. The generator detects when the power grid resumes operation and within five (5) minutes, restores power to the grid and shuts down the generator. This added redundancy virtually guarantees seamless and continuous power to the data centers. Additionally, to assure that all services are continuously maintained in the event of a major disruption to the two-piece GPS data centers, Sentinel provides full system backup in the event of a power loss or natural disaster, Sentinel monitoring center is outfitted with the latest state-of-the-art technology including:

			▪ Fault tolerant central computer system offering maximized uptime. ▪ APC Symetra battery back-up Uninterruptible Power Supply (UPS). ▪ Kohler 150kVA diesel generator. Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that, during normal electrical power operation, provides filtered and regulated power to all of the monitoring center's components. The UPS unit serves to protect all computers and electronic equipment from unexpected power spikes or surges that can damage components. If a power outage does occur the UPS continues to power the entire monitoring center as normal and can do so for up to 60 minutes. This is more than sufficient power capability as Sentinel's on-site diesel generator automatically begins operation within 30 seconds upon registering a power outage. There is no memory loss due to the fact that Sentinel's on-site generator initiates service within one (1) minute of commercial power loss. Once operating, Sentinel's generator can provide power for the entire monitoring center for up to 10 days or longer if refueled. The diesel generator is regularly inspected to ensure that it remains in operational order at all times.
3.4	Data Center	The Vendor must have redundant Data Centers located a sufficient distance apart in the event of a disaster of the local area.	**Sentinel exceeds this requirement.** The proposed one-piece GPS data storage system is highly redundant and secure in its operation and system failure protocols and is 100% redundant, having completely redundant, identical and live systems **more than 500 miles apart. All data centers maintain the same data in real time and can immediately take over operation of the entire operation at any time.** Live hardware and software engineers supervise the system 24 hours a day, seven (7) days and week, 365 days a year to ensure the best possible uptime. The data centers are both certified: ▪ ISO9001 ▪ SAS-70 Audited ▪ HIPPA Certified SunGard's Managed Services Facilities provides redundant, co-located, high-availability and IT related managed services including data-replication, storage and security for mission-critical technology needs. SunGard uses the term "redundant system" to describe a primary system with a back-up system rated at 100% of the capacity of the primary system. To support business operations for the proposed two-piece GPS system for

			database replication of key IT, and failover disaster recovery, Sentinel's monitoring system incorporates redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring and data center is located in California, its back-up monitoring center and redundant DRP servers are located in Atlanta, Georgia, **over 500 miles apart**. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full on-site and full off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a manmade or natural event the causes major disruption to electrical or communications services to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred.
3.5	Data Center	All back-up systems in the Data Centers must be tested regularly.	**Sentinel exceeds this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing its monitoring centers, all of the proposed systems data centers and the company's ability to continue meeting customer needs while coping with circumstances than might arise during a disaster. Sentinel customizes its Risk Mitigation and Disaster Recovery Plan to each agency upon contract award and will provide this plan to any requesting agency post award. All revisions/updates to this plan will be forwarded to the agency as they occur. **Disaster and Recovery testing is done regularly on both systems to ensure full operations in the event of a technology disaster, systems failure or network outage.** Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. **Should a period of failover occur, there would be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred.**
3.6	Data Center	The Vendor's system must provide for 100% redundancy to avoid unnecessarily excessive downtime due to hardware or software issues. In the event of data	**Sentinel exceeds this requirement.** Sentinel's primary monitoring center is equipped with an Uninterruptible Power Supply (UPS) that serves to immediately protect all computers and electronic equipment from downtime continuing to power the entire monitoring center as normal and can do so while

		disruption, the secondary Data Center must be activated within 10 minutes of initial system failure.	Sentinel's on-site diesel generator automatically begins operation. Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's ability to continue meeting customer needs on all monitoring solutions while coping with circumstances than might arise during a disaster. Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs within the corrections industry. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. **Regardless of the cause, Sentinel's contingency plans will failover in the case of any system malfunction that effects participant monitoring or reporting, which cannot be corrected within 10 minutes of the initial system failure.** The one-piece GPS data storage system is highly redundant and secure in its operation and system failure protocols and is 100% redundant, having completely redundant, identical and live systems more than 500 miles apart. **All Data Centers maintain the same data in real time and can immediately take over operation of the entire operation at any time.** Live hardware and software engineers supervise the system 24 hours a day, seven (7) days and week, 365 days a year to ensure the best possible uptime. SunGard's Managed Services Facilities provides redundant, co-located, high-availability and IT related managed services including data-replication, storage and security for mission-critical technology needs. SunGard uses the term "redundant system" to describe a primary system with a back-up system rated at 100% of the capacity of the primary system. To support business operations for the proposed two-piece GPS system for database replication of key IT, and failover disaster recovery, Sentinel's monitoring system incorporates redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring and data center is located in California, its back-up monitoring center and redundant DRP servers are located in Atlanta, Georgia, **over 500 miles apart**. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee maximum uptime performance to receive, store and disseminate data from the field.

			Redundant web servers, application servers and database servers are present at both sites. RAID disk arrays are employed in both sites providing high data availability. Databases are mirrored between the two (2) sites providing both hardware redundancy for component failure as well as disaster recovery. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. Sentinel uses an industry standard data protection and recovery software package to ensure that the databases within the primary and back-up data servers are concurrently maintained, which ensures the following: ▪ No loss of data from the databases if there is a failover ▪ Capability for the back-up database to immediately and automatically become available for processing and access The system maintains a constant connection between the primary and back-up database servers and when it detects the loss of a regular "heartbeat" signal between the systems, it automatically initiates an alert notifying Sentinel of this loss. It is then determined if the loss of heartbeat was an anomaly or it is warrants a real-time failover from the primary database server to the back-up server.
3.7	Data Storage	The Vendor must ensure that all records (automated or hard copy files) remain the property of the Agency and upon request shall be returned within 30 days, in the event the contract is canceled or terminated.	**Sentinel meets this requirement.** All records created for GPS tracking participants referred to this program by any participating agency will remain solely the property of the participating agency. Upon completion of services, all records (automated or hard copy files) will be returned to the participating agency within 30 days or destroyed under direction of agency staff.
3.8	Data Storage	The Vendor's system must ensure that all data be recorded with a historical transaction record and stored/archived for retrieval/backup in a database when requested by Agency personnel in accordance with the following:	**Sentinel meets this requirement.** Both proposed GPS tracking solution's computer software system databases immediately and automatically (in real-time) record with a historical transaction records all of the data received by the monitoring equipment, entered at the time of enrollment, data and/or monitoring changes, monitoring reports and terminations exchanged between officers and the monitoring center facility. Additionally, the system databases store/archive for retrieval/backup all monitoring data so that all authorized users

			can view or exchange monitoring and tracking data, such as enrollment, curfew assignment or changes, caseload review, reports and terminations, with the proposed Sentinel monitoring platform using secure access.
3.9	Data Storage	a. All historical data must be centrally stored and accessible for reporting purposes;	**Sentinel meets this requirement.** When data is received from for the proposed GPS tracking solutions, it is centrally stored in Sentinel data centers and accessible through the SenTrak the web-based application. This central information hub houses all offender data and allows courts and supervising agencies to access and manage their data from any web-based browser.
3.10	Data Storage	b. This information must be available for reporting in a standard transaction file format; and	**Sentinel meets this requirement.** Authorized users have the ability to directly access all participant historical information through Sentinel's SenTrak computer software system databases. All monitoring reports are available through the proposed software's easy-to-use report generator applications in a standard transaction file format.
3.11	Data Storage	c. All current and historical data files must be retained for a minimum period of seven (7) years and this information shall be available at no charge to the Agency.	**Sentinel exceeds this requirement.** Sentinel secures all GPS tracking system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. SunGard's Managed Services Facilities provides redundant, co-located, high-availability and IT related managed services including data-replication, storage and security for mission-critical technology needs for Sentinel's proposed one-piece GPS tracking solution. SunGard uses the term "redundant system" to describe a primary system with a back-up system rated at 100% of the capacity of the primary system. Additionally, all key information is backed up daily on tape and destroyed only when the customer submits a request. The two-piece GPS solution databases are backed up on removable discs, using the industry recognized Symantec Backup Exec software data back-up and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel. If system recovery is necessary, Sentinel is not limited to the sole use of back-

			ups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler. Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups.
3.12	Data Storage	The Vendor's Data Centers must have duplicate computers with the ability to, at a minimum, permit restoration of data collection and user monitoring services within ten (10) minutes after computer failure. The Monitoring Center must have duplicate data storage devices with automated fail-over and automatic re-establishment of the duplicate databases upon replacement of the failed storage device.	**Sentinel exceeds this requirement.** The workstations and central computer systems within Sentinel's monitoring/data centers are equipped with redundant features designed to perform the same monitoring functions. They are all "ghosted" or duplicate workstations that process the incoming signals similarly. If one of the computers is not functioning properly, all incoming signals are simply routed **immediately** to one of the other available computers. In addition, Sentinel employs internal Information Technology personnel. In the event that a computer, facsimile or modem error occurs, Sentinel's IT personnel quickly replace the computer component with no affect on the alarm processing capabilities of the entire system. Along with spare computer workstations, Sentinel has additional equipment available to replace facsimile machines, modems and all other monitoring center components thus allowing seamless operation of the monitoring/data center at all times. The one-piece GPS server platform was specifically designed with redundancy and uptime in mind. T he system is divided into the following layers: ▪ Web UI Layer ▪ Application Layer ▪ Database Layer ▪ Location Server Layer Each layer is doubly and in some instances, triply redundant. There are load balancers that run between each layer, allowing information to be distributed between systems so if there is a problem in any layer or maintenance needs to be done, the system can be rectified easily with no lapse in service. Additionally, Sentinel secures all two-piece GPS system data so it can be re-created should the system fail or the data corrupts. Sentinel's system architecture is designed to provide regular and reliable data backups while the system remains online and available. Databases are backed up on removable discs, using the industry recognized Symantec Backup Exec software data back-up and disaster recovery software package. The discs are encrypted to ensure security of the data stored in a secure, off-site location. Sentinel makes full

			backups daily and incremental backups every hour. Encrypted backups are sent off-site and kept in a secure l fireproof storage facility which is located 30 miles away for one (1) month. Month end backups are sent off-site to be archived for a period of 12 months and year end backups are sent off-site to be archived for seven (7) years. Transportation of backup media in locked containers to and from the backup facility and the Sentinel monitoring center and is performed only by authorized personnel. **If system recovery is necessary, Sentinel is not limited to the sole use of back-ups, as it images the key permanent elements of the system upon installation, including the web server, database server and call handler.** Imaging allows the server's operating system, and key applications and setting to be re-created without the requirement for a full rebuild, facilitating a rapid recovery. Once imaged, system databases are restored from the most recent backups.
3.13	Data Storage	Upon request from the Agency, 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 to be determined by the Agency.	**Sentinel meets this requirement.** Upon request, Sentinel will provide the most up-to-date complete copy of the respective agencies monitoring data included in 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 the participating agency and in a manner that will not compromise overall confidentiality and system integrity.
3.14	Data Access	The Vendor shall not release or reveal any GPS data, program information, operation protocols, implementation plans, training material, report(s), publication(s), updates, and/or statistical data related to the GPS Program to any entity, to include non-GPS Agency personnel, without prior written approval from the Agency Program Manager.	**Sentinel meets this requirement.** At no time will Sentinel ever disclose confidential data including 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 any unauthorized personnel without written approval of the participating agency Program Manager. All program data will be maintained in accordance with secure data protection standards. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel.

			Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.15	Data Access	The Vendor must maintain unaltered recorded data of offender violations, to be accessible in original form and substance for utilization as physical evidence for prosecution.	**Sentinel meets this requirement.** The proposed GPS tracking solutions' database systems maintain unaltered recorded data of offender violations, accessible in their original form and substance for utilization as physical evidence for prosecution. Sentinel tracks **all** changes to the application, including but not limited to participant or agency details, notes, alert resolutions, enrollments, terminations and service requests.
3.16	Security	The Vendor's Data Centers must have on-site in-person security 24 hours a day, 7 days per week. The system shall provide security features, which prevent unauthorized individuals from accessing any information held by the Vendor. Secure access to the system shall be maintained at all times.	**Sentinel meets this requirement.** **Physical Security:** The one-piece GPS data centers use state-of-the-art technology and best practices for securing both the facility and the data. The data center is staffed features four (4) physical layers of security, including but not limited to **24 hours a day, seven (7) days a week on-site staffing from dedicated security and storage engineers**; access doors that are monitored and alarmed for tamper protection; all of the environmental control alarms are connected into the main security panel located at the security desk and the onsite Network Operations Center (NOC); state-of-the-art access card system; trained security personnel; closed circuit television cameras (CCTV) that record and monitor activity both inside and outside the facilities, and biometric and key card security. The data center for the two-piece GPS monitoring system resides in Sentinel's **continuously staffed, independently secured monitoring center facility**. To maintain monitoring center operational integrity, each shift must complete the Facility Check List to ensure that systems and alarms are functional throughout the facility. Sentinel restricts access to authorized staff and enforces an electronic key card system for entryway access to both outside building and monitoring center and as uses multiple security systems (including active video/audio systems, alarms system, and motion and fire detectors monitored by an outside security contractor) for supervising the entryways. **Security of Monitoring Records:** In Sentinel's experience with offender populations nationwide, Sentinel understands the importance of data integrity both in its actual data entry as well as its subsequent data retention. To ensure that the proper information is entered at all times, Sentinel's personnel are thoroughly trained on data entry procedures with supervisorial support for any adjustments or corrections. Each user is given their own login and once they set

			their confidential password Sentinel can ensure the integrity of each user's entry. This unique user access allows Sentinel's Information Technology personnel to follow electronic audit trails that allow supervisors and management to verify the source of all date entry. The workstations that Sentinel's staff and agency personnel use at the monitoring center and/or local facilities are technically only used to connect to Sentinel's central server systems. **Note:** No offender data is stored on-board any office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. In addition, Sentinel's monitoring center, data centers and secure web-based monitoring system incorporates the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel. A System Performance Monitor continuously scans the monitoring center platforms and displays live diagnostics of all routers, servers, modems and Internet connections into the corporate center. Within 30 seconds of any failure the system monitors mounted at supervisor's workstations audibly and visually indicate a malfunction. Monitoring center staff are trained in recovery procedures and restart systems according to procedure. Sentinel's Engineering Department, in conjunction with Sentinel's IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system malfunction, and ensure continued operations. Any instance of failure resulting in a loss of monitoring capability will be reported to the participating agency. Sentinel's redundant server and communications platforms have allowed it to deliver continuous service without an interruption to Sentinel's monitoring services. All of Sentinel's security systems are monitored continuously. **Monitoring System Security:** Upon program enrollment, Sentinel provides security passwords and unique login names to each user. The system has the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses.

			To prevent unauthorized access from outside the monitoring and/or center, the software uses leading Internet security features, including 128-bit encryption. The proposed monitoring platform uses Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Sentinel also employs multiple firewalls designed to keeps outside computer users from interfering with the internal network operations and to also keep them from retrieving private information from other network computer systems. Sentinel utilizes a firewall appliance that is regularly monitored and reviewed to be sure that the appliance is properly functioning and to monitor unauthorized activity.** The firmware (software) that is running on the appliance is regularly updated to ensure Sentinel has the latest security technology patches, fixes, and updates and that they are properly applied. The appliance monitors all Internet traffic that goes in and out of the monitoring servers, to and from its ultimate destination to ensure that the data / traffic is adhering to the set rules that are in place on the Internet Firewall appliance. All of the firewall and/or remote access dial-in connections will stop any messages they are not specifically told to allow. **Personnel Security: Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will

			remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.17	Security	The Vendor must maintain security policies and procedures for its network security, application security, data transmission security, data storage security, and physical security. While it is not necessary for the vendor to submit these documents with proposal, they must be provided to any requesting agency post award.	**Sentinel meets this requirement.** Sentinel maintains security policies with its Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, monitoring center/data center physical security for each of the proposed solutions. (Please note: Each of these items have been fully addressed previously in this section). Additionally, Sentinel's maintains ISO 9001-2008 accreditation for the provision of electronic monitoring services to ensure the establishment of quality objectives throughout its departments including all layers of security. Sentinel has provided copies of the certifications in the Exhibits section of this proposal. Post award upon request, Sentinel will supply an requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
3.18	Security	The Vendor shall provide secure transmission and storage of GPS data and must ensure that all data, data transmissions and data storage is kept confidential.	**Sentinel meets this requirement.** Sentinel provides secure transmission and storage of all monitoring data and has policies and procedures in place to ensure that all data, data transmissions and data storage is kept confidential. **Network and Data Transmission Security:** To prevent unauthorized access from outside the monitoring and/or data center, the software uses leading Internet security features, including 128-bit encryption. Both the proposed monitoring platforms use Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions. **All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each Sentinel employee has a specific database login credential that allows Sentinel to perform detailed audits on user access to all records in the database to confirm if unauthorized changes have been made.** **Application Security:** Upon program enrollment, Sentinel provides security

			passwords and unique login names to each user. The proposed systems have the capability to limit officer access to his or her caseload status or be flexible enough to provide tiered level access for senior level staff with all officer and participant information and statuses. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. **Data Security:** Sentinel's monitoring center, data centers and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that Sentinel handles daily, Sentinel has taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are Sentinel's main concern. Sentinel manages this through its System Performance Monitoring and Security against unauthorized personnel/intrusion. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency. **Personnel Security: Only authorized personnel have access to offender**

			data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards. The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the courts. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
3.19	Security	The Vendor's facility, equipment, data transmissions, and data storage shall be secure. At a minimum, the Vendor's facility shall be alerted and monitored by a local law enforcement Agency or security company. The alert line shall be a tamper-resistant dedicated circuit and shall not be exposed to any person or thing that could alter or damage the line. The Monitoring Center shall be equipped with automated fire detection and suppression equipment.	**Sentinel meets this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, monitoring center/data center physical security for each of the proposed solutions. (Please note: Each of these items have been fully addressed previously in this section). The one-piece GPS data center uses state-of-the-art technology and best practices for securing both the facility and the data. Water detection is provided under the raised floor area. In addition, the Vesda System, which is an extremely sensitive air sampling system, is used as an early warning of any smoke or very early pre-ignition conditions. All fire suppression alarms are monitored at the security panel located at the security desk. At the two-piece GPS data center, Sentinel uses multiple security systems including active video/audio systems, alarms system and motion and fire

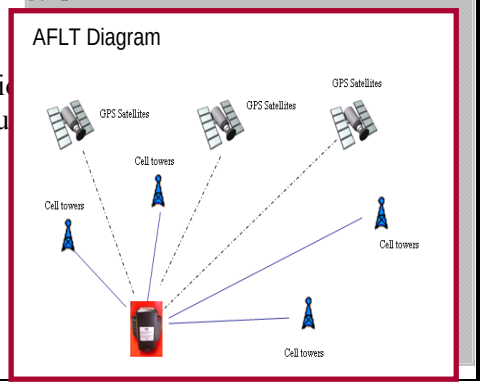
			detectors that are monitored by an outside security contractor for supervising the entryways into the facility. The outside security contractor will alert Sentinel each time there is a potential security threat through a tamper-resistant dedicated circuit that is secured against any person or thing that could alter or damage the line. Additionally the continuously staffed Sentinel monitoring and data centers resides in an independently secured, facilities with raised floors, a fire detection and suppression systems and written policies and procedures for access that meet all applicable federal, state and local regulations regarding safety.
3.20	Security	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 any requesting agency post award.	**Sentinel meets this requirement.** Sentinel has a developed and tested comprehensive Risk Mitigation and Disaster Recovery Plan addressing the company's network security, application security, data transmission and data security, monitoring center/data center physical security for each of the proposed solutions as well as its plan to maintain continuous operations in the event of power failures, telephone system failures, local equipment failures, flood or fire at the monitoring center and/or data centers (Please note: Each of these items have been fully addressed previously in this section). Post award and upon request, Sentinel will supply an requesting participating agency with a **CONFIDENTIAL** copy of its comprehensive Risk Mitigation and Disaster Recovery Plan.
4a.0	**SECTION D Equipment Requirements – single body-attached device**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
4a.1	Equipment	Vendor is bidding the following one-piece body-attached device and the accessories identified in the Price Worksheets. The responses to these specifications are for this equipment. **One-piece Body-attached Device:** Mfg.: _____ Brand/Model: _____	**Sentinel meets this requirement.** **One-piece Body-attached Device:** Mfg.: Omnilink Systems, Inc. Brand/Model: OM series Please refer to the letter of support from executives at this manufacturer pledging their support to Sentinel for this WSCA contract and additionally confirming >500 units in use with Sentinel government customers.
4a.2	Equipment	The Vendor shall provide, at their own expense, all systems and equipment	**Sentinel meets this requirement.** Sentinel will provide each WSCA participating agency, at no additional cost, direct access to all systems and

		(software and hardware) required for the service delivery, regardless of the actual number of units including but not limited to:	equipment (software and hardware) required for the service delivery, regardless of the actual number of units utilized through this contract. As a leading provider of monitoring services throughout the industry, Sentinel has spent more than 20 years servicing offender monitoring programs nationwide. Sentinel operates some of the largest programs in the country exceeding 1,000 offenders while simultaneously supporting agencies using less than five (5) active devices. Sentinel is prepared to continue providing service to agencies of differing sizes and is pleased to present the **OM Series One-Piece GPS** solutions to Western States Contracting Alliance and its participating agencies. Sentinel is pleased to propose the OM210 and OM400 that are each one-piece, single unit devices that are also each the receiver of location information and the transmitter of status and location information supported by the innovative, user-friendly web-based information exchange, SenTrak. The OM series one-piece devices do not require a base or docking station, or landline communications. The following list highlights some of the unique features of the proposed OM series GPS tracking solution: OM series ▪ **Unique Location Technology:** The OM210 GPS location-tracking device was the first device on the market to utilize Advanced Forward Link Trilateration (AFLT) in addition to GPS to monitor participants. ▪ **Impaired Locate:** Each OM series device reliably provides location monitoring from a single device in impaired environments where GPS alone does not work, for example, in the participant's home, as well as areas outside the home such as the car floorboards, shopping malls, buildings, buses, etc. ▪ **Most Accurate GPS Points:** The OM series devices feature the proprietary "Precision Engine" generating the most accurate GPS points available. ▪ **Decreased Loss Rates:** The OM series one-piece design and unique location technology provides the lowest loss rate for devices in the

			industry. ▪ **Reduction in False Alerts:** Compared to other electronic monitoring and GPS systems, officers will spend far less time working with the equipment and responding to "false positive alerts" leading to increased efficiency and productivity. ▪ **Truly Safe Device:** The proposed device is truly 100% waterproof, safe to the wearer, engineered for heavy-duty shock resistance and FCC, CE, ROHS, IC and SAR compliant. ▪ **Easiest Installation Process:** The proposed device is the easiest one-piece GPS device to install in the industry, no tools or strap cutting are needed. The OM series units work out of the box each time and the GPS acquisition time is less than 60 seconds. ▪ **Widely Variable Intensity Rate Plans:** The proposed device allows agency staff to match monitoring intensity with level of supervision needed within the field. This capability provides tremendous cost savings. ▪ **Long Battery Life:** The OM series tracking systems feature one of the longest battery lives at the most intense monitoring levels and does not require the participant to carry extra batteries, car chargers, home units or phone lines. The batteries also have rapid charging capability. ▪ **Triple Layer Tamper Detection:** The proposed device has an adjustable, replaceable hypoallergenic strap with a tamper evident locking mechanism and multi-level tamper detection including 1) strap tamper, 2) device tamper and 3) device removal. ▪ **Mobile Exclusion Zones:** Staff will have the ability to create mobile exclusion zones around a victim by providing the victim with his or her own OM series device. The agency determines the size of any zone. ▪ **Victim and Gang Member Tracking:** The OM series unit can track monitored gang members or victims (carrying a device) in relation to program participants to provide needed proximity alerts. This capability is of significant value to expand the notification capabilities to victims of domestic violence that have restraining orders in place. ▪ **Buffer Zones:** The agency will have the unique ability to create buffer zones around fixed or mobile exclusion zones to alert participants of an upcoming potential violation. ▪ **Crime Scene Report Query**: WSCA agencies will have the ability to locate multiple GPS participants via proximity to any location or crime scene.
4a.3	Equipment	a. A system with a database to monitor	**Sentinel meets this requirement.** Today, Sentinel provides service to more

		offender activity;	than 60,000 offenders utilizing some of the most advanced monitoring and case management software systems in the industry. SenTrak, Sentinel's proprietary software, is utilized to perform all GPS tracking services. **Using this system, all agencies and authorized personnel, have real-time, online access to participant monitoring activity and information.** Sentinel internally developed the software and provides all scheduled maintenance to ensure that the system remains in optimal operational status at all times. Authorized personnel using SenTrak can view and print monitoring activity reports at any time. SenTrak also has the ability to notify the designated person immediately upon receipt of any tracking information to the monitoring center. Simultaneously, SenTrak can distribute alerts to multiple locations/persons. The ability to parse data and customize the automated process makes the minimum processing time mere seconds.
4a.4	Equipment	b. All monitoring units (transmitter, receiver/dialer and other related equipment) to communicate location data to the Vendor's system;	**Sentinel meets this requirement. The OM series devices are single unit devices; each are both the receiver of location information and the transmitter of status and location information.** The OM210 device communicates over the Sprint mobile broadband network as the primary wireless provider and the OM400 offers added cellular diversity via the Verizon network. OM series devices will automatically roam to other CDMA cellular networks if a viable Sprint/Verizon signals are not available. Virtually **any CDMA cellular service can provide service to the OM series**.
4a.5	Equipment	c. All software and hardware required to access the Internet, with the exception of Agency personal computers; and	**Sentinel meets this requirement.** Sentinel's proprietary software, SenTrak, is a web-based system that provides a user-friendly interface for offender enrollment, scheduling, and communication. Sentinel's internal Information Technology (IT) department developed, owns and operates the SenTrak system, providing in-house maintenance expertise as well as total control over the database, data field queries, reports and overall operations. Authorized personnel have the capability to use SenTrak software to enroll new offenders and view the latest activity and violation information. Authorized personnel using SenTrak can view and modify offender curfew schedules and view and print monitoring activity reports. SenTrak also allows agency personnel to make notes about offender-generated alerts. All these features are available in real-time, any time, and anywhere via a totally web-based system. SenTrak is accessible over the Internet by authorized personnel, through secure connections and password-protected interfaces. **Sentinel customers do not**

			need to purchase or download any custom hardware or software. Upon program enrollment, Sentinel assigns security passwords and unique login names to SenTrak users. **As a web-based system, SenTrak does not require any special software, plug-ins, or hardware for access by designated personnel.** Sentinel's IT staff has installed all of the necessary physical and technical security measures (i.e., SSL certificates, network firewalls, anti-virus software, access control equipment, and closed-circuit television) to ensure that unauthorized users and hackers do not have access to SenTrak or the monitoring center.
4a.6	Equipment	d. All labor, materials, equipment, cellular wireless service costs and consumables necessary to perform GPS tracking services on an as-needed basis.	**Sentinel meets this requirement.** Sentinel understands the importance of providing the necessary personnel, materials, equipment, cellular wireless service costs, and consumables associated with performing GPS tracking services and will do so if awarded.
4a.7	Equipment	All equipment and systems furnished shall be standard products supplied by the Vendor, shall be in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.	**Sentinel meets this requirement.** Sentinel is an authorized reseller of the OM series GPS tracking systems, a standard product supplied by Sentinel and in fact has a "private label" arrangement for OM series equipment distributed through Sentinel. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. **Sentinel employs a Quality Assurance Plan that includes a Final Quality Checklist to the ensure that all initial and new equipment shipment leave the warehouse in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.**
4a.8	Equipment	The Vendor shall provide only equipment that meets the highest levels of ruggedness, durability and performance available, when considering the following: operating temperature, stored temperature range, temperature cycling, shock and vibration, water resistance or waterproofing, operating humidity range, stored humidity range and tamper resistance.	**Sentinel exceeds this requirement.** The proposed OM series one-piece GPS tracking devices are in service on more than 8,000 thousand offenders nationwide. The OM series meets the highest standards in equipment durability and performance and have passed pass rigorous testing for temperature, shock, water resistance and tamper capabilities. For example, the OM series tracking solution equipment has been designed to meet or exceed the following standards: Feature: OM210 Durability Standard Stored/Operating Temperature: -68° F to 140° F Temperature Cycling: No restriction within stored /operating temperature limits

			Shock/Vibration: 500 MHz of random vibration of 1.25G rms Water: 100% Waterproof in fresh and salt water to a depth of 50 feet Operating Humidity Range: Relative humidity of less than 95% Stored Humidity Range: Relative humidity of less than 95% Tamper Resistance: Multi-level tamper detection, Fiber optic cable tamper resistant strap, Tamper evident locking mechanism
4a.9	Equipment	The device shall be a one-piece body-attached device. Performance information and product literature may be included in Vendor's proposal response.	**Sentinel meets this requirement.** The OM210 and OM400 devices are each a single unit device that are both the receiver of location information and the transmitter of status and location information. The proposed device is truly 100% waterproof, safe to the wearer, engineered for heavy-duty shock resistance and FCC, CE, ROHS, IC and SAR compliant. The OM series tracking system features one (1) of the longest battery lives at the most intense monitoring levels and does not require the participant to carry extra batteries, car chargers, home units or phone lines. The batteries also have rapid charging capability. Additionally, an OM series device is the easiest one-piece GPS device to install in the industry, no tools or strap cutting are needed. The proposed device has an adjustable, replaceable hypoallergenic strap with a tamper evident locking mechanism and multi-level tamper detection including 1) strap tamper, 2) device tamper and 3) device removal. The OM series works out of the box each time and the GPS acquisition time is less than 60 seconds. The OM series one-piece designs and unique location technology provides the lowest loss rate for devices in the industry. **Unique Location Technology:** In additi has secondary location technologies inclu Forward Link Trilateration (AFLT). GPS alone does not reliably work in some impaired environments such as 

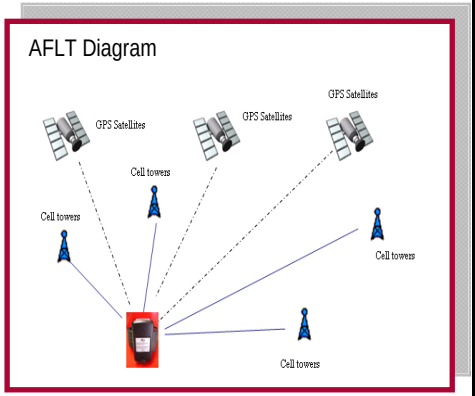
			home, car floorboards, buildings, buses and/or other weak satellite locations. Unique to the OM series device is the utilization of **Advanced Forward Link Trilateration (AFLT)**, GPS and Assisted GPS to locate the unit. This enhanced dual-monitoring feature allows reliable location tracking from a single device even in impaired environments. AFLT triangulates utilizing ambient longitude and latitude data advertised in the environment. Sprint and Qualcomm employ this technology to locate cell phone users who dial 911. In ideal conditions, the OM series acquires a GPS signal within 60 seconds and provides virtually continuous real-time location data of monitored participants. When the device registers no GPS signal, the **OM series device's AFLT will provide the agency unmatched confidence that the device is reliably monitoring the participant's location.** Older technologies that use standalone GPS alone cannot do this and will not track participants in areas where GPS is impaired (for example: inside buildings) but OM series devices will. **Most Accurate GPS Points:** Additionally, the OM series device utilizes Assisted GPS and AFLT to determine participant locations and the proposed software features the proprietary "Precision Engine" software that automatically maximizes the accuracy of the multiple location technologies into one (1) point, generating one (1) of the most accurate GPS points available. **Widely Variable Intensity Rate Plans:** The OM series device, through its supporting software, provides the flexibility an agency needs for controlling the level of supervision each participant receives to meet individual monitoring needs and budget constraints. This level is defined by the type of monitoring assigned in the participant's risk profile. The risk profile not only defines the monitoring intensity, but also allows the agency to change the level, based on a participant's current monitoring status. Risk profiles available include, but are not limited to active, hybrid and passive risk profiles: **Reduction in False Alerts:** Compared to other electronic monitoring and GPS systems, officers will spend far less time working with the equipment and responding to "false positive alerts" leading to increased efficiency and productivity. The OM series devices offer the most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. The devices remain in tamper until inspected and reset through the SenTrak software. The reduction in excessive tamper events that are a nuisance to officers reduces tamper events to only those that truly warrant investigation and necessitate oversight. If an officer is not

			near a computer, he or she may call the Sentinel monitoring center to clear any tamper event. For each tamper event, officers can program multiple notifications, such as reminders.
4a.10	Equipment	The Vendor shall provide equipment that meets market safety standards and presents no health or safety hazards to staff and/or offenders.	**Sentinel exceeds this requirement.** The OM series devices do not pose a health or safety hazard to participants or agency staff, exceeds market safety standards, are manufactured to SARS and ISO 9000 standards, and are certified by the FCC. **IMPORTANT SENTINEL ADVANTANGE:** In addition to the proposed devices being manufactured in ISO certified facilities, Sentinel is ISO 9001:2008 certified as an electronic monitoring provider and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations and monitoring center including agency/departmental specific operational procedures.
4a.11	Equipment	The device identified by the Vendor above shall be the latest proven reliable technology and meet the requirements specified in Items 1.2 and 1.3 above.	**Sentinel exceeds this requirement.** Sentinel is proposing its latest generation, most advanced OM series GPS and SenTrak software, which have been in continuous use for more than four (4) years in agencies nationwide and has been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for the OM series GPS tracking solution in the Appendix D: Bidder Information and Profile section of this proposal and additionally in the response to Item 1.2 as required
4a.12	Equipment	The device shall not have any sharp edges and shall be designed so not to cause excessive chafing or bruising.	**Sentinel meets this requirement.** The small and inconspicuous OM210 device's dimensions are 3.5 X 1.5 X 1.75 inches and it weighs 5.3 ounces. The OM400 has the same dimensions, yet approximately ¼ inch thicker to allow for advanced features of audible/vibration/visual alert and acknowledgment button capabilities incorporated within this device. Both are designed with rounded edges so as not to cause any discomfort, chafing or bruising to the participant while being worn. The strap and backplate used to attach the OM series are hypoallergenic.
4a.13	Equipment	The device shall use Global Position Satellites and the cellular telephone network to track and report the location(s) of offenders both at home and in the community, regardless of location. Passive, Hybrid, and Active devices must be the same one-piece body-attached device securely attached to the ankle.	**Sentinel exceeds this requirement.** The OM series devices are each a single unit device that is both the receiver of location information and the transmitter of status and location information. The OM series devices do not require a base or docking station, or landline communications and each OM series device is fully capable of functioning in active, passive and hybrid GPS tracking modes. Any one OM series device, **through the supporting software without changing equipment,** provides the flexibility an agency needs for controlling the level of supervision each participant receives to meet individual monitoring

needs and budget constraints including passive, hybrid, and active tracking capabilities in the the same one-piece body-attached device securely attached to the ankle.

In addition to the use of GPS, the OM series devices have secondary location technologies including **Assisted GPS and Advanced Forward Link Trilateration (AFLT) to determine participant locations and the proposed software features the proprietary "Precision Engine" software that automatically maximizes the accuracy of the multiple location technologies into one point, generating one of the most accurate GPS points available.**

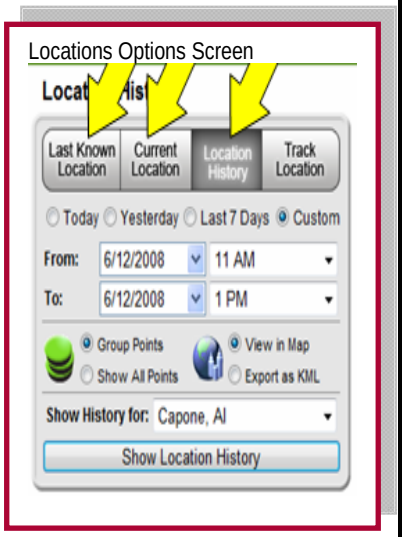
IMPORTANT SENTINEL ADVANTAGE: The OM series has secondary location technologies including Assisted GPS and Advanced Forward Link Trilateration (AFLT). GPS alone does not reliably work in some impaired environments such as the participant's home, car floorboards, buildings, buses and/or other weak satellite locations. Unique to the OM series device is the utilization of **Advanced Forward Link Trilateration (AFLT)**, GPS and Assisted GPS to locate the unit. This enhanced dual-monitoring feature allows reliable location tracking from a single device even in impaired environments. AFLT triangulates utilizing ambient longitude and latitude data advertised in the environment. Sprint and Qualcomm employ this technology to locate cell phone users who dial 911. In ideal conditions, the OM series acquires a GPS signal within 60 seconds and provides virtually continuous real-time location data of monitored participants. When the device registers no GPS signal, the **OM series device's AFLT will provide the agency unmatched confidence that the device is reliably monitoring the participant's location.** Older technologies that use GPS alone cannot do this and will not track participants in areas where GPS is impaired (for example: inside buildings) but OM series devices will.



The OM210 device communicates over the Sprint mobile broadband network as the primary wireless provider and the OM400 offers added cellular diversity via the Verizon network. OM series devices will automatically roam to other

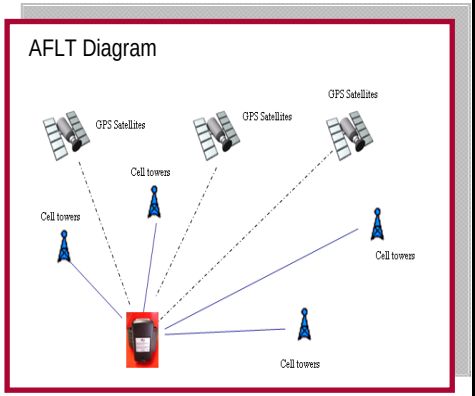
			CDMA cellular networks if a viable Sprint/Verizon signals are not available. Virtually **any CDMA cellular service can provide service to the OM series**.
4a.14	Equipment	Active GPS shall be a service level that must collect a tracking point at least once every minute, and must report information via 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.	**Sentinel exceeds this requirement.** In active tracking mode, Sentinel's OM series GPS tracking solution collects a tracking point or location once every minute. **Alerts such as tamper are report immediately. Compliant events and tracking points are reported via the cellular network to the monitoring center system at least every 15 minutes.** **IMPORTANT SENTINEL ADVANTANGE: In the event of an alert condition and regardless of the mode of operation, the OM series devices will report the alert immediately, further the device will automatically increase its transmission frequency to a one (1) minute GPS point, one (1) minute impaired locate through AFLT and a one (1) minute transmission of monitoring data under alert conditions.** The OM series devices have the capability to change the frequency of monitoring automatically when an exclusion zone has been breached. When an exclusion zone is breached several things occur. First, an exclusion zone alert is sent out immediately as directed by agency to users supervising the participant. Second, the device reverts into "constant tracking" mode. While in constant tracking mode, the device will use all three (3) location methods (GPS, Assisted GPS and AFLT via cellular tower triangulation) to determine and report locations in real time. It will remain in this mode until the device leaves the exclusion zone or the battery is exhausted. **In addition, users can add a buffer zone around an exclusion zone for added safety.** Buffer zones may or may not be alert situations as defined by the agency user, but if a buffer zone is entered, the constant tracking mode is activated to track the participant more accurately and to "catch" them entering the exclusion zone with greater reliability.
4a.15	Equipment	Passive GPS shall be 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.	**Sentinel exceeds this requirement.** In passive tracking mode, Sentinel's OM series GPS tracking solution collects a tracking point or location once every minute. **The tracking points are then reported via the cellular network to the monitoring center system at least every 12 hours.** **IMPORTANT SENTINEL ADVANTANGE: In the event of an alert condition and regardless of the mode of operation, the OM series devices will report the alert immediately, further the device will automatically increase its transmission frequency to a one (1) minute GPS point, one (1) minute impaired locate through AFLT and a one (1) minute transmission**

			of monitoring data under alert conditions. Additionally, the OM series devices have the capability to change the frequency of monitoring automatically when an exclusion zone has been breached regardless of the mode of operation. When an exclusion zone is breached several things occur. First, an exclusion zone alert is sent out immediately as directed by agency to users supervising the participant. Second, the device reverts into "constant tracking" mode. While in constant tracking mode, the device will use all three (3) location methods (GPS, Assisted GPS and AFLT via cellular tower triangulation) to determine and report locations in real time. It will remain in this mode until the device leaves the exclusion zone or the battery is exhausted. In addition, users can add a buffer zone around an exclusion zone for added safety. Buffer zones may or may not be alert situations as defined by the agency user, but if a buffer zone is entered, the constant tracking mode is activated to track the participant more accurately and to "catch" them entering the exclusion zone with greater reliability.
4a.16	Equipment	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.	**Sentinel exceeds this requirement.** Sentinel offers multiple hybrid service plans in addition to the multiple active and passive service plans described in the previous two (2) specification responses. In hybrid tracking mode, Sentinel's OM series GPS tracking solution collects a tracking point or location once every minute. **Alerts such as tamper are report <u>immediately</u>. Compliant events and the tracking points are then reported via the cellular network to the monitoring center system as frequently as every 30 minutes.** **IMPORTANT SENTINEL ADVANTANGE: In the event of an alert condition and regardless of the mode of operation, the OM series devices will report the alert immediately, further the device will automatically increase its transmission frequency to a one (1) minute GPS point, one (1) minute impaired locate through AFLT and a one (1) minute transmission of monitoring data under alert conditions.** Additionally, the OM series devices have the capability to change the frequency of monitoring automatically when an exclusion zone has been breached regardless of the mode of operation. When an exclusion zone is breached several things occur. First, an exclusion zone alert is sent out immediately as directed by agency to users supervising the participant. Second, the device reverts into "constant tracking" mode. While in constant tracking mode, the device will use all three (3) location methods (GPS, Assisted GPS and AFLT via cellular tower triangulation) to determine and report locations in real time. It will remain in this mode until the device leaves the exclusion zone or the battery is exhausted. In addition, users can add a buffer zone around an exclusion zone for added safety. Buffer zones may or

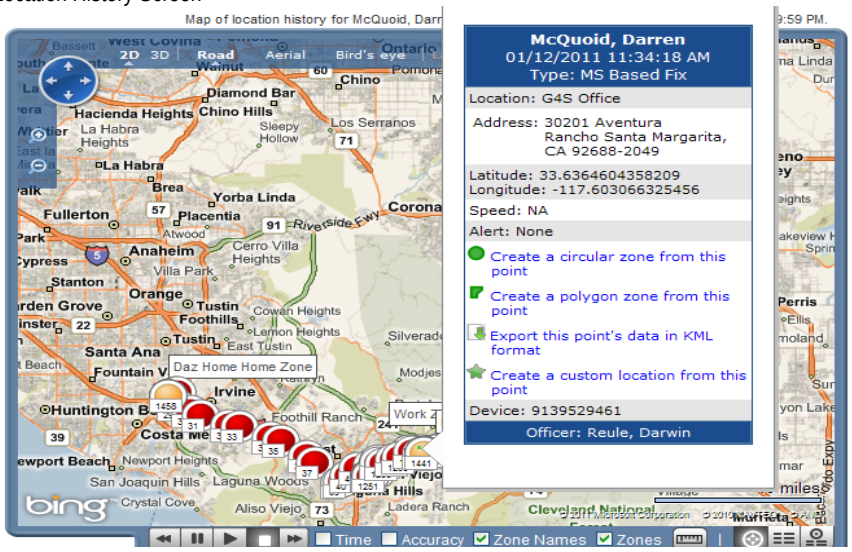
			may not be alert situations as defined by the agency user, but if a buffer zone is entered, the constant tracking mode is activated to track the participant more accurately and to "catch" them entering the exclusion zone with greater reliability.
4a.17	Equipment	Active GPS includes the ability of the device to be remotely contacted to force the device to instantly locate and call back with its data immediately. Vendor shall include unlimited instant cellular locates at no additional costs.	**Sentinel meets this requirement.** Since the OM series devices are always active and communicate through cellular coverage, authorized users will have the ability to perform on-demand location verifications ("Instant Locates"). In fact, the web-based software enables agencies to view Last Known Location and Location History as well as Current Location. Real-time participant information, including on-demand location verifications, can be accessed through the software Location History window "Current Location" button as shown to the right. While this on-demand location information is accessed at the time of request virtually instantaneously, Last Known Location gives the user the fastest information, taking the last point stored and displaying it on the map. The time of the point is given, along with the relative address and latitude and longitude. If more current information is needed, selecting Current Location will instruct the software to contact the device, perform an immediate location and display it on the map.  **Sentinel has included unlimited Instant Locates in its pricing at no additional costs.**
4a.18	Equipment	All devices must be capable of utilizing unlimited alternative location tracking using the cellular network in the absence of GPS at no additional costs.	**Sentinel exceeds this requirement.** In addition to the use of GPS, all OM series devices have secondary location technologies including **Assisted GPS and Advanced Forward Link Trilateration (AFLT) to determine participant locations.** **PLEASE NOTE: The AFLT functionally remains active for all OM series monitoring levels at all times.** Some other vendors (BI, Inc.) will claim their device is "AFLT compatible" but in fact do not include this feature in their pricing and ultimately supply devices to agencies with the AFLT feature tuned-off.

Additionally, the proposed software features the proprietary "Precision Engine" software that automatically maximizes the accuracy of the multiple location technologies (GPS, Assisted GPS and/or AFLT) into one point, generating one of the most accurate GPS points available.

IMPORTANT SENTINEL ADVANTAGE: The OM series has secondary location technologies including Assisted GPS and Advanced Forward Link Trilateration (AFLT). GPS alone does not reliably work in some impaired environments such as the participant's home, car floorboards, buildings, buses and/or other weak satellite locations. Unique to the OM series device is the utilization of **Advanced Forward Link Trilateration (AFLT)**, GPS and Assisted GPS to locate the unit. This enhanced dual-monitoring feature allows reliable location tracking from a single device even in impaired environments. AFLT triangulates utilizing ambient longitude and latitude data advertised in the environment. Sprint and Qualcomm employ this technology to locate cell phone users who dial 911. In ideal conditions, the OM series acquires a GPS signal within 60 seconds and provides virtually continuous real-time location data of monitored participants. When the device registers no GPS signal, the **OM series device's AFLT will provide the agency unmatched confidence that the device is reliably monitoring the participant's location.** Older technologies that use GPS alone cannot do this and will not track participants in areas where GPS is impaired (for example: inside buildings) but OM series devices will.



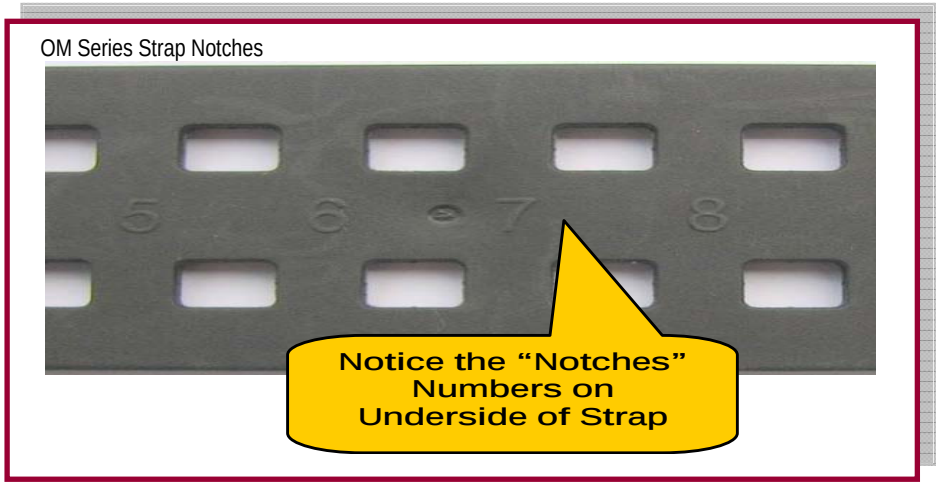
IMPORTANT SENTINEL ADVANTAGE: In an effort to compete, other vendors offering devices exclusively on the GSM network(s) (incompatible with Sprint's or Verizon's AFLT) have begun to promote cleverly worded alternatives such as "TBT – Tower Based Tracking" (3M), "Layered Location Capability" (Satellite tracking of People "STOP"), and "Advanced Secondary Location Tracking (ASLT)" These alternatives do NOT truly provide enhanced tracking but rather only provide secondary shaded areas indicative of the location of cellular towers that the GPS device is communicating that could be

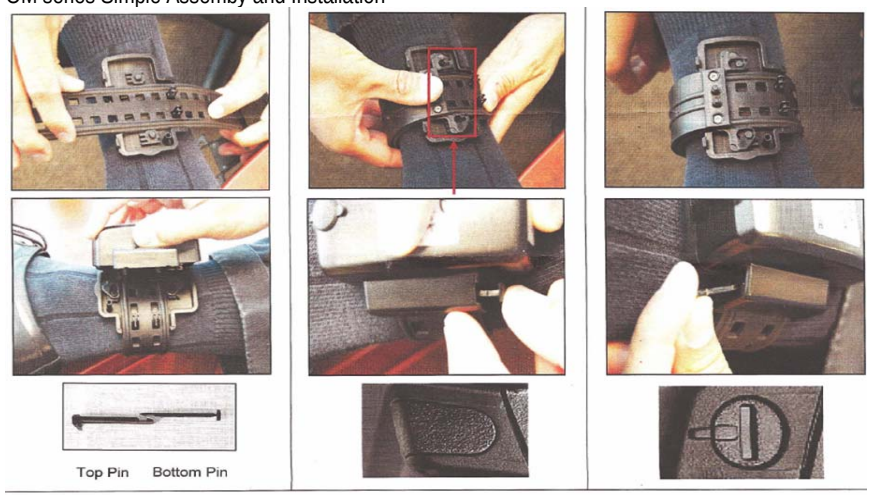
			miles away and not indicative of the area in which the actual tracking device is located. These alternatives result in officers having to compare the primary tracking points to these secondary shaded areas and then having to make a best guess to determine the location accurately. These factors are widely known by the most experienced GPS users and can be verified through the reference checks as part of this RFP evaluation.
4a.19	Equipment	Describe how the web based system reflects the alternative tracking verses GPS tracking and how the location indicators on the map differentiate between the two.	**Sentinel exceeds this requirement. IMPORTANT SENTINEL ADVANTAGE:** The Sentinel proposed "Precision Engine" GPS software automatically maximizes the accuracy of the multiple location technologies **(GPS, Assisted GPS and/or AFLT) into one/the same point, generating one of the most accurate GPS points available.** Tracking points are differentiated by color according to ageny and numbered in order of occurrence. Additionally by hovering over any point on the location history screen, the SenTrak software will display the name of the participant, the date and time of the location point and the type of point that was acquired at the top of the pop-up-box as shown in the following screen. Location History Screen 
4a.20	Equipment	The system shall have the capacity to convert a device between active and passive mode without removal from the Offender or requiring a change of	**Sentinel exceeds this requirement.** The OM series devices are each a single unit device that is both the receiver of location information and the transmitter of status and location information. The OM series device, **through its supporting software without removal or changing of equipment,** provides

<table>
<tr>
<td></td>
<td></td>
<td>equipment.</td>
<td>the flexibility an agency needs for controlling the level of supervision each participant receives to meet individual monitoring needs and budget constraints. This level is defined by the type of monitoring assigned in the participant's risk profile. The risk profile not only defines the monitoring intensity, but also allows the agency to change the level, based on a participant's current monitoring status. Risk profiles available include, but are not limited to:
<table>
<tr><th>Risk Profile</th><th>Mode of Operation</th></tr>
<tr><td>Active Monitoring</td><td>Acquires a GPS point every 60 second increments and automatically transmits data every 15 minutes. Tampers are immediately transmitted.</td></tr>
<tr><td>Hybrid Monitoring</td><td>Acquires a GPS point every 60 seconds and automatically transmits data every 30 minutes. Tampers are immediately transmitted.</td></tr>
<tr><td>Passive Monitoring</td><td>Acquires a GPS point every 60 seconds and automatically transmits data every 12 hours minutes. Tampers are immediately transmitted.</td></tr>
</table>
Any authorized user can change a participant's risk profile at any time during monitoring. For example, an officer may initially assign a participant with a passive monitoring profile for low risk monitoring, but determine the need to increase the monitoring intensity to active monitoring if the participant has recurring violations. In contrast, if an officer determines during a participant's monitoring timeframe that the participant poses less risk to the community than originally observed, the officer can easy modify that participant's risk profile from active monitoring to passive monitoring. Any single OM series device can be software controlled to operate at increased and decreased intensities, allowing for real-time monitoring changes without the need to have contact with the participant or the monitoring equipment.</td>
</tr>
<tr>
<td>4a.21</td>
<td>Equipment</td>
<td>The device shall be small, light, and not restrictive and can be attached to the offender in a manner that will not impede normal activities or work. It shall attach securely around the ankle of the offender.</td>
<td>Sentinel meets this requirement. The OM series devices are easily attached around the ankle of participants and do not unduly restrict a participant's physical activities. OM210 device's dimensions are 3.5 X 1.5 X 1.75 inches and it weighs 5.3 ounces. The OM400 has the same dimensions, yet approximately ¼ inch thicker to allow for advanced features of audible/vibration/visual alert and acknowledgment button capabilities incorporated within this device. The devices are extremely easy to securely attach to the participant's ankle with a reusable, adjustable and replaceable strap. The strap includes a permanently embedded fiber-optic cable and is fully adjustable, eliminating the need for strap cutting during installation. Two (2) locking pins connect the unit to the</td>
</tr>
</table>

			back plate. Personnel installing an OM series on the participant need **no tools**. The installer will connect the device to the ankle of a participant with only their thumb and forefinger. Once properly attached, the device will detect and report a tamper message if it is removed. When properly installed, attempts to defeat, remove or tamper with the OM series will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The back plate fits precisely in place and any attempts to pry it open are easily noticeable.
4a.22	Equipment	The device shall not pose a safety hazard nor unduly restrict offenders' activities.	**Sentinel meets this requirement.** The OM series devices are non-metallic, do not pose a safety hazard to participants, are manufactured to SARS and ISO 9000 standards and are certified by the FCC.
4a.23	Equipment	All equipment assigned to the offender shall be manufactured to allow for repeated proper sanitization. The Vendor shall provide instructions to sanitize the equipment, including recommended cleaning agents and methods.	**Sentinel meets this requirement.** The OM series device and strap are easily sanitized and reusable on multiple participants without the need for replacement. Each device is manufactured for use on multiple offenders and therefore designed to withstand normal and repeated cleaning practices. Additionally, both the OM series device and strap are dishwasher safe, which is the easiest and safest way to sterilize the devices or may be cleaned with disposable, antibacterial pop-up wipes. During the training process, authorized personnel will be provided with written instructions and trained on the recommended cleaning methods and products best suited for thorough sanitation.
4a.24	Equipment	The device components are quickly removable by a trained officer and are not easily removable except by an officer with the correct equipment.	**Sentinel meets this requirement.** Sentinel's transmitter has been designed for ease of removal and durability. Using a standard screwdriver, provided at no cost to the agency, the officer will remove the locking pins on either side of the device and separate the GPS device from the backplate and strap. Removal of the OM series device by a trained officer takes only seconds to complete. **Please note:** While the design of the OM series device allows for easy officer removal, the strap includes a permanently embedded fiber-optic cable **that will immediately detect if the offender is attempting to remove the device**. Once the OM series is properly installed, it cannot be removed unless the strap is cut or the device itself is damaged. Any attempt to cut the strap or damage the device (e.g., remove the backplate) will generate a tamper alarm.

4a.25	Equipment	All communications to and from the device shall be encrypted.	**Sentinel meets this requirement.** All communications from the OM series GPS tracking device the monitoring center are encrypted. Sentinel has used these products on thousands of offenders and has not experienced any breach in security of the offender records due to communications.
4a.26	Equipment	The device shall 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.	**Sentinel exceeds this requirement.** Sentinel will include at least one (1) tool kit for each 25 units in use, including an installation kit containing all necessary equipment to install, activate or deactivate the device. Personnel installing an OM series device on the participant need **no tools for installation**. The installer will connect the device to the ankle of a participant with only their thumb and forefinger then place two (2) locking pins to connect the unit to the back plate. Once properly attached, the device will detect and report a tamper message if it is removed. Sentinel staff will enroll a participant in the SenTrak application. The enrollment process is quick, simple and completed in five (5) to 10 minutes by entering basic data and selecting the respective officer. Upon a participant's enrollment, the installer will fit a sanitized unit on the participant through a straightforward configuration process which consists of 1) adjusting the strap to the participant's ankle, 2) securing the device on the participant, 3) changing the status of the device to active and 4) assigning the device to the participant on the web-based platform, SenTrak. The software recognizes the device as soon as it is activated and assigned to the participant, providing confirmation that the device is working properly.

4a.27	Equipment	The device shall be simple to install and have easy to understand instructions.	**Sentinel meets this requirement.** The OM series are simple to install and have easy to understand instructions. Personnel installing an OM series device on the participant need **no tools**. The installer will connect the device to the ankle of a participant with only their thumb and forefinger then place two (2) locking pins to connect the unit to the back plate. The OM series strap's design allows for a secure fit and has multiple holes to assist in finding the proper fit on each person. The strap is adjustable as needed prior to locking the pins in place to allow the participant to stand up and/or walk around to determine the best fit possible. The next two (2) pictures illustrate the sizing of the strap followed by an installation diagram: 

			OM Series Fit to Ankle OM series Simple Assemby and Installation 
4a.28	Equipment	The device shall be permanently marked with the model/serial identification numbers and will withstand exposure to common cleaning products. The vendor will replace any device without charge if the tracking number is not legible.	**Sentinel meets this requirement.** Prior to distribution, each unit is permanently marked with a unique serial number of the unit that can withstand exposure to common cleaning products as well as daily bathing by the offender. The label also provides a toll free "Reward if Found" telephone number. Sentinel utilizes a bar code system on each and every product shipped from its warehouse. In addition, this serial number is placed on a bar code sticker that is

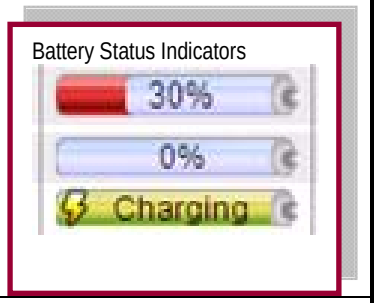
			securely attached to the unit. Utilizing the bar code and bar code scanner, Sentinel is able to track equipment as it moves between customer sites and Sentinel's warehouse location. Sentinel understands the need to replace any device if the serial number is no longer legible and agrees to comply with this requirement at no additional charge.
4a.29	Equipment	The device shall be capable of tracking an offender twenty-four (24) hours a day, 7 days a week and shall be able to confirm the date, time and location of the tracking event.	**Sentinel meets this requirement.** The OM series GPS tracking solution is specifically designed for the criminal justice industry and provides reliable, continuous 24 hour a day, seven (7) day a week, 365 day a year offender tracking via GPS technology. Through the OM series, Sentinel offers intensive tracking of offenders at one point per minute at all levels of tracking and records and stores each point with the date, time and location of the event for use in monitoring a participant's compliance with court orders and terms/conditions of probation.
4a.30	Equipment	The device and all additional equipment shall not be available as an open market item if this could compromise the security of the system.	**Sentinel meets this requirement.** The OM series GPS tracking solutions are specifically designed for the criminal justice industry. Sentinel's OM series GPS tracking solution features non-commercially available devices in order to maintain the security of the system and the reliability of the participant's monitoring.
4a.31	Equipment	The strap and circuitry shall enable the device to immediately notify the Monitoring Center of any tamper attempt or removal from the offenders' ankle.	**Sentinel exceeds this requirement.** The OM series units detect three (3) tamper types including 1) strap tamper, 2) device tamper and 3) device removal. Within one (1) second of a tamper attempt, the device will communicate and send a unique alert to the SenTrak web interface. **The OM series device will automatically and <u>instantly</u> communicate to the SenTrak software when a participant attempts to remove or tamper with the strap.** The SenTrak system then immediately sends the alert to the appropriate agency defined personnel. The elapsed time for a device tamper to be executed and then have a notification via text message and/or voice call is under 45 seconds. The OM series devices will send a tamper alert if the participant severs the strap or if the unit loses contact with the back plate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit. When properly installed, attempts to defeat, remove or tamper with the OM series will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The back plate fits precisely in place and any attempts to pry it open are easily noticeable. **IMPORTANT SENTINEL ADVANTAGE:** The OM series devices offer the

<table>
<tr><td></td><td></td><td></td><td>most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. The devices remain in tamper until inspected and reset through the SenTrak software. The reduction in excessive tamper events that are a nuisance to officers reduces tamper events to only those that truly warrant investigation and necessitate oversight. If an officer is not near a computer, he or she may call the Sentinel monitoring center to clear any tamper event. For each tamper event, officers can program multiple notifications, such as reminders.</td></tr>
<tr><td>4a.32</td><td>Equipment</td><td>The device shall acquire GPS within 5 minutes when placed in an outdoor environment.</td><td>Sentinel exceeds this requirement. Sentinel confirms its OM series tracking devices will acquire GPS within five (5) minutes when placed in an outdoor environment. Upon activation, installers will NOT need to stand outside with the OM series device to obtain GPS signal due to its secondary location technology, Advanced Forward Link Trilateration (AFLT).

IMPORTANT SENTINEL ADVANTAGE: Additionally, the OM series device is designed to also assist the installers to confirm proper installation/enrollment the following event:

<table><tr><th>Events</th><th>Description</th></tr><tr><td>Initial GPS Success</td><td>Occurs when the device first establishes GPS after being assigned to a participant.</td></tr></table></td></tr>
<tr><td>4a.33</td><td>Equipment</td><td>The battery for the device shall hold a single charge for a minimum period of sixteen (16) hours while performing one minute GPS acquisition and downloading data to the Database System at least once every 15 minutes.</td><td>Sentinel exceeds this requirement. The OM series GPS tracking device has an intensive monitoring battery up-time of 24 hours (active) to 60 hours (passive) depending upon the rate plan used by the agency far exceed the requirement of 16 hours while performing one minute GPS acquisition and downloading data to every 15 minutes demonstrating the superior performance of the OM series GPS tracking solution.</td></tr>
<tr><td>4a.34</td><td>Equipment</td><td>The device shall be shock-resistant.</td><td>Sentinel meets this requirement. The OM series GPS tracking device are shock-resistant and can withstand up to 500 MHz of random vibration of 1.25G rms of shock.</td></tr>
<tr><td>4a.35</td><td>Equipment</td><td>The device’s battery shall 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 a maximum capacity (100% charge) in two (2) hours or less.</td><td>Sentinel exceeds this requirement. Participants charge the OM series GPS tracking device through a standard 110V plug with a 15-foot cord easily connected directly to the front of the unit. The unit has an intensive monitoring battery up-time of 24 hours (active) to 60 hours (passive) depending upon the rate plan used by the agency. These devices feature a rapid recharge capability to allow recharge from completely dead in 1.5 hours.

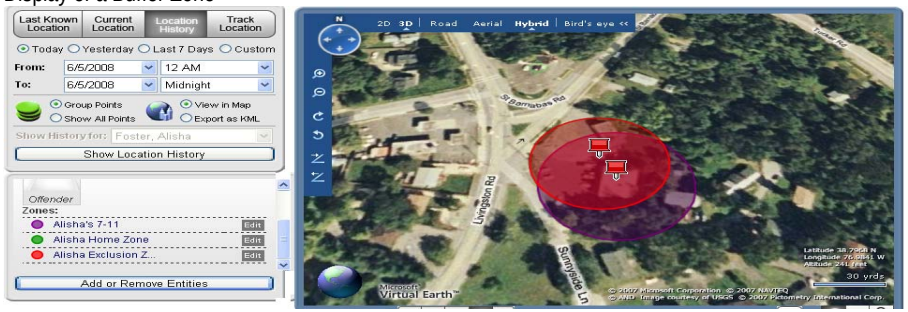
IMPORTANT SENTINEL ADVANTAGE: The device reports the battery status each time it reports to the monitoring center. If the device’s power is</td></tr>
</table>

			low, the monitoring center will generate a low battery alert. A low battery alert is generally generated when the device is at 40% or less of battery power. This alert will clear when battery power is restored above 85%. To mitigate low battery issues, agencies can incorporate a mandatory recharging schedule into the participant's daily schedule. If the device is not charging at the scheduled time, or if it is unplugged prior to the expiration of the charging schedule, the monitoring center will send an alert to the assigned officer or contact the offender and instruct he or she to recharge the device. 
4a.36	Equipment	The battery powering the transmitter shall have a guaranteed life cycle of not less than twelve (12) months. Each device shall be replaced at specific intervals to avoid device failures due to loss of battery power.	**Sentinel exceeds this requirement.** The OM series device features an internal battery that boasts the industry's longest battery life of **12 to 18 months in-use with a shelf life of three (3) years**. Sentinel understands the importance of ensuring that all agencies utilizing the OM series tracking devices have the ability to replace the devices at specified intervals in order to avoid failures due to a loss of battery power. Therefore, each OM series is tracked through Sentinel warehouse and Asset Management software to ensure replacement occurs **prior to battery failure.**
4a.37	Equipment	The device shall 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.	**Sentinel exceeds this requirement.** Participants charge the OM series GPS tracking devices through a standard 110V plug with a **15-foot cord** that is easily connected directly to the front of each unit. An optional automobile outlet (direct current) source to recharge battery is available at no additional charge if requested by the agency.
4a.38	Equipment	The device shall have internal diagnostics that can determine if it is operating properly and the ability to relay the information to the Vendor's Monitoring Center.	**Sentinel meets this requirement.** The OM series GPS tracking devices are designed to continuously monitor functionality and report proper operability. In addition to the internal diagnostics including location capability and battery condition performed by the unit itself, the SenTrak software is constantly requiring communication and thus the lack of those scheduled contacts is reported immediately in accordance with agency established notification guidelines. **All OM series alerts, as determined by agency notification protocols, can be processed automatically and immediately in real-time** upon receipt of the violation information to the monitoring system. The proposed system will notify the designated officers immediately in real-time when the following **alerts occur and are cleared** for participants on one-piece GPS monitoring when there is a operation or communication disturbance.

Notification Alerts	Alert Generated/ Cleared	Description
Commun-ication Failure	System Generated	Occurs if device is unsuccessful in communicating with Sprint for two consecutive intervals according to the set Communication Failure System Generated rate plan. The device will attempt to use the cellular network two (2) times and then will start a 45 minute timer. If it is still unable to contact Sprint during this timeframe, a communication failure alert is generated.
	Auto or Manually Cleared	This condition may be cleared by the user or by the system when the device is able to obtain a Sprint signal again. If data is saved in the device's memory, it is sent at this time.
Location Failure	System Generated	Occurs when the device is not able to obtain its location. This alert automatically clears through the software
	Auto or Manually Cleared	Occurs when the device is able to obtain its location and the system or user clears the alert.
Low Battery	System Generated	Automatic system generated message that occurs when the device reaches 40% of remaining battery power.
	Auto or Manually Cleared	Automatically clears when the device has been recharged to 80% or more.
Recharge Schedule Alert	System Generated	Occurs when a participant misses their mandatory recharge schedule. Creating a battery recharge schedule is optional and managed by the software administrator.
	Auto or Manually Cleared	Occurs when the Recharge Schedule alert is cleared by the user.

<table>
<tr><td></td><td></td><td></td><td>IMPORTANT SENTINEL ADVANTAGE: Additionally, the OM series device is designed to also assist the installers to confirm proper installation/enrollment as well as participant compliance through the following events:
<table>
<tr><th>Events</th><th>Description</th></tr>
<tr><td>Initial GPS Success</td><td>Occurs when the device first establishes GPS after being assigned to a participant.</td></tr>
<tr><td>Recharge Begin</td><td>Occurs when a participant successfully plugs in their device. Once the participant has charged the device, the device will locate every 20 minutes minimum. If they are on a rate plan that is greater than 20 minutes then they will obtain location points per their specified rate plan.</td></tr>
<tr><td>Recharge End</td><td>Occurs when a participant disconnects the charging cord from their device.</td></tr>
<tr><td>Insufficient Charging Time</td><td>A system generated message that automatically records when a participant charges their device for less than an hour.</td></tr>
</table></td></tr>
<tr><td>4a.39</td><td>Equipment</td><td>The device shall be designed to prevent tracing or duplication of the signal by other electronic devices or equipment.</td><td>Sentinel meets this requirement. The OM series GPS tracking devices are designed to prevent tracing or duplication of the signal by other electronic devices or equipment. Additionally, all communications from the OM210 GPS tracking device the monitoring center are encrypted to prevent both confidentiality breach and duplication/tracing of monitoring information. Sentinel has used these products on thousands of offenders and has not experienced tracing or duplication of the signal by other electronic devices or equipment.</td></tr>
<tr><td>4a.40</td><td>Equipment</td><td>The device and software system should be capable of storing up to 99 zones so that zone violations can be immediately reported regardless of the call in frequency.</td><td>Sentinel exceeds this requirement. The SenTrak web-based monitoring software system will allow authorized users to create, edit and delete all parameters for individual participants. Users can create unlimited individual monitoring schedules as well as unlimited inclusion and exclusion zones for each participant. Additionally, the system will allow approved staff the ability to apply monitoring schedules and zones for entire groups of participants.

The OM series device also has the capability to change the frequency of monitoring automatically when an exclusion zone has been breached. When an exclusion zone is breached several things occur. First, an exclusion zone alert is reported to the monitoring software and then sent out immediately as directed</td></tr>
</table>

			by agency to users supervising the participant. Second, the device reverts into "constant tracking" mode. In this mode, the device will use all three (3) location methods (GPS, Assisted GPS and AFLT via cellular tower triangulation) to determine and report locations in real time. It will remain in this mode until the device leaves the exclusion zone or the battery is exhausted. In addition, users can add a buffer zone around an exclusion zone for added safety. Buffer zones may or may not be alert situations as defined by the agency user, but if a buffer zone is entered, the constant tracking mode is activated to track the participant more accurately and to "catch" them entering the exclusion zone with greater reliability. **IMPORTANT SENTINEL ADVANTAGE:** The system provides the ability to create buffer zones around exclusion zones. Buffer zones can be attached to an exclusion zone and can be set at a 50-foot minimum radius with no maximum limit. Once a device is in a buffer zone, the device will automatically activate a constant tracking mode (get location information once every minute and report into the system once every minute) regardless of the participant's monitoring type until the device is located outside of the buffer zone. This capability allows agencies to more accurately track participants entering the exclusion zone with greater reliability. Display of a Buffer Zone 
4a.41	Equipment	The device shall communicate to the Vendor's Software System by common cellular carrier, with the option of a secondary cellular carrier (list cellular networks proposed).	Sentinel exceeds this requirement. The OM series devices do not require a base or docking station, or landline communications and are fully capable of functioning in active, passive and hybrid GPS tracking modes. The OM series devices are one-piece rugged GPS tracking units that are each, both the receiver of location information and the transmitter of status and location information supported by Sentinel's web-based information exchange.

			The OM series devices communicate with the monitoring center via the largest cellular footprint in the country. The OM210 tracking device utilizes CDMA technology and the wireless services **Sprint**, and the OM400 offers added cellular diversity via the Verizon network two (2) of the largest cellular carriers in the country. Moreover, the OM series tracking device will automatically **"Roam" on any CDMA available service provider** which has lead to increased coverage capabilities nationwide.
4a.42	Equipment	The device shall be waterproof, and has been independently tested against the effects of continuous immersion in water.	**Sentinel meets this requirement.** The OM series has undergone extensive testing to ensure its waterproof casing is able to withstand the rigors associated with submersion not only in bathing situations but also in swimming and hot tub scenarios. The OM Series' device casing is hardened and waterproof against the effects of continuous immersion to a depth of 50 feet in both salt water and fresh water. The OM series' battery is enclosed directly inside the device casing. This eliminates problems with removable batteries found in other one-piece GPS devices, where moisture can enter the inner components through the battery insertion area thereby compromising the overall functionality of the device.
4a.43	Equipment	The device may be able to detect and record an alert feature to signal the offender by audible tone or vibration method. Describe your available features.	**Sentinel meets this requirement. The OM400 incorporates advanced alert features for audible/visible/vibration participant signal alert/communication** and an on-board acknowledgment button incorporated within this device. The SenTrak software enables officers to pre-profile on a per-participant basis, the event types that will trigger these audible/visible/vibration participant signal alert/communications. Additionally, officers can trigger signal the offender on-demand from the SenTrak software. .
4a.44	Equipment	The device shall be able to detect and record an alert feature with immediate tamper notification.	**Sentinel exceeds this requirement.** The OM series unit detects three (3) tamper types including 1) strap tamper, 2) device tamper and 3) device removal. Within one (1) second of a tamper attempt, the device will communicate and send a unique alert to the SenTrak web interface. **The OM series device will automatically and instantly communicate to the SenTrak software when a participant attempts to remove or tamper with the strap.** The SenTrak system then immediately sends the alert to the appropriate agency defined personnel. The elapsed time for a device tamper to be executed and then have a notification via text message and/or voice call is under 45 seconds. The proposed monitoring software offers a continuum of user-defined officer/user alerts and notifications. **For each participant alert, an unlimited number of people including administrators, officers, police, victims and judges can be sent notifications.** Alerts can be delivered via SMS text message, automated voice call, page (numeric or alpha-numeric), e-mail and/or

fax. Privacy rules can be configured to ensure all participant and user data is kept confidential. The agency can set instantaneous response, end of day notification summary or no notification requirements. Sentinel will work with the staff to ensure all notifications are customized to meet personnel schedules, set work day hours, off time, etc. to guarantee the appropriate response times to ensure public safety.

In fact, **all OM series alerts, as determined by agency notification protocols, can be processed automatically and immediately in real-time** upon receipt of the violation information to the monitoring system. The proposed system will notify the designated officers immediately in real-time when the following **alerts occur and are cleared** for participants on one-piece GPS monitoring when there is a tamper violation.

Notification Alerts	Alert Generated/ Cleared	Description
Device Tamper	System Generated	Occurs if the participant attempts to remove /disassemble the device. This alert must be manually cleared through the web based software.
	Manually Cleared	Occurs after the device tamper condition has been corrected and the user clears the Device Tamper manually through the web based software.
Strap Tamper	System Generated	Occurs when the participant attempts to cut, remove or tamper with the strap attached to the device. This alert must be manually cleared through the web based software.
	Manually Cleared	Occurs when a strap tamper is cleared by the user through the web based software.

The OM series devices offer the most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. **The devices remain in tamper until inspected and are reset through the SenTrak software.** The reduction in excessive tamper events that are a nuisance to officers reduces tamper events to only those that truly warrant investigation and necessitate oversight. If an officer is not near a computer, he or she may call the Sentinel monitoring center

			to clear any tamper event. For each tamper event, officers can program multiple notifications, such as reminders. **IMPORTANT SENTINEL ADVANTAGE: Automatic reset is an outdated approach commonly used by vendors whose equipment experiences a high volume of false tamper alarms and consequently, by automatically resetting, makes it highly prone for a tamper to be overlooked if the band is re-closed as it will automatically reset. Advanced GPS devices such as the OM series devices have been developed that do not suffer from false tampers, thus the device stays in tamper until evaluated by an officer, then can be reset via the web-based system or via remote data device (such as BlackBerry).**
4a.45	Equipment	The device or system shall be able to detect and record an alert feature with immediate alert notification for inclusion and/or exclusion zone violations.	**Sentinel exceeds this requirement.** In fact, Sentinel exceeds this requirement as **all OM series alerts, as determined by agency notification protocols, can be processed automatically and immediately in real-time** upon receipt of the violation information to the monitoring system. The proposed system will notify the designated officers immediately in real-time when the following **alerts occur and are cleared** for participants on one-piece GPS monitoring when there is a exclusion zone violation,, from an inclusion zone violation or buffer zone violation.

Notification Alerts	Alert Generated / Cleared	Description
Exclusion Zone Alert	System Generated	Occurs when a participant is in violation of his schedule by entering a user defined zone that is prohibited.
	Auto or Manually Cleared	Occurs when a participant has left a prohibited zone and the alert is cleared by the system or by the user.
Inclusion Zone Alert	System Generated	Occurs when a participant leaves a user defined zone they are required to remain within during scheduled times.
	Auto or Manually Cleared	The system will automatically clear this alert if the participant returns to the inclusion zone during the scheduled time. If the participant does not return to the inclusion zone during the scheduled time, the user must manually

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td><td>clear this alert through the web based software.</td></tr>
<tr><td>Buffer Zone Alert</td><td>System Generated</td><td>Occurs when the participant enters a user defined zone. A buffer zone is an extra distance that can be attached to an exclusion zone and can be set at 50 foot minimum radius with no maximum limit. Once a device is in a buffer zone, it will automatically get assigned a one minute rate plan until the device is located outside of the buffer zone then resume its normal plan.</td></tr>
<tr><td></td><td>Auto or Manually Cleared</td><td>Occurs when the participant exits the buffer zone attached to the exclusion zone.</td></tr>
</table>
</td></tr>
<tr><td>4a.46</td><td>Equipment</td><td>The device shall be able to detect and report and alert feature with immediate alert notification for loss of communication violations.</td><td>
Sentinel exceeds this requirement. In fact, Sentinel exceeds this requirement as all OM series alerts, as determined by agency notification protocols, can be processed automatically and immediately in real-time upon receipt of the violation information to the monitoring system. The proposed system will notify the designated officers immediately in real-time when the following alerts occur and are cleared for participants on one-piece GPS monitoring when there is a loss of communication with the monitoring center.
<table>
<tr><th>Notification Alerts</th><th>Alert Generated / Cleared</th><th>Description</th></tr>
<tr><td>Commun-ication Failure</td><td>System Generated</td><td>Occurs if device is unsuccessful in communicating with Sprint for two consecutive intervals according to the set Communication Failure System Generated rate plan. The device will attempt to use the cellular network two (2) times and then will start a 45 minute timer. If it is still unable to contact Sprint during this timeframe, a communication failure alert is generated.</td></tr>
<tr><td></td><td>Auto or Manually Cleared</td><td>This condition may be cleared by the user or by the system when the device is able to obtain a Sprint signal again. If data is saved in the device's memory, it is sent at this time.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>4a.47</td><td>Equipment</td><td>The device shall be able to detect and record an alert feature with immediate alert notification for a low battery.</td><td>

Sentinel exceeds this requirement. In fact, Sentinel exceeds this requirement as **all OM series alerts, as determined by agency notification protocols, can be processed automatically and immediately in real-time** upon receipt of the violation information to the monitoring system. The proposed system will notify the designated officers immediately in real-time when the following **alerts occur and are cleared** for participants on one-piece GPS monitoring when there is an low battery condition.

<table>
<tr><th>Notification Alerts</th><th>Alert Generated/ Cleared</th><th>Description</th></tr>
<tr><td rowspan="2">Low Battery</td><td>System Generated</td><td>Automatic system generated message that occurs when the device reaches 40% of remaining battery power.</td></tr>
<tr><td>Auto or Manually Cleared</td><td>Automatically clears when the device has been recharged to 80% or more.</td></tr>
<tr><td rowspan="2">Recharge Schedule Alert</td><td>System Generated</td><td>Occurs when a participant misses their mandatory recharge schedule. Creating a battery recharge schedule is optional and managed by the software administrator.</td></tr>
<tr><td>Auto or Manually Cleared</td><td>Occurs when the Recharge Schedule alert is cleared by the user.</td></tr>
</table>

</td></tr>
<tr><td>4a.48</td><td>Equipment</td><td>The device may be able to detect and record an alert feature with-alert notification to detect potential masking of the device's ability to receive GPS signals.</td><td>

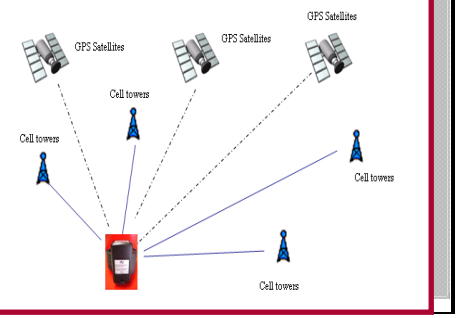
Sentinel meets this requirement. Upon the basis that the OM series is constantly tracking via <u>both</u> cellular AFLT and GPS, it is extremely rare for a device to be successfully masked from both signals. In such an event both GPS and cellular signals are blocked and the agency will receive a continued <u>combination</u> of <u>both</u> "No GPS" <u>and</u> "No Communication" alerts. This simultaneous combination is indicative of the potential of a masked device. In these circumstances, Sentinel and/or the agency can contact the participant to investigate and/or instruct the participant on remedial steps to un-mask the device.

</td></tr>
<tr><td>4a.49</td><td>Equipment</td><td>As an optional feature, identify and describe any offender acknowledgement feature located on the device.</td><td>

Sentinel meets this requirement. The OM400 incorporates advanced alert features for audible/visible/vibration participant signal alert/communication and **an on-board acknowledgment button incorporated within this device**. The SenTrak software enables officers to pre-profile on a per-participant basis, the event types that will trigger these audible/visible/vibration participant signal alert/communications. Additionally, officers can trigger signal the offender on-

</td></tr>
</table>

			demand from the SenTrak software.
4a.50	Equipment	The device should incorporate non-volatile memory capable of storing at least 24 hours worth of events (with date and time of occurrence) at times when the cellular service or electrical power may become unavailable. Non-volatile memory will retain unreported events and report them once power/cellular services have been restored, including date & time of occurrence.	**Sentinel exceeds this requirement.** The OM210 features an internal memory to store approximately 24 hours worth of events and the OM400 has expanded memory capabilities to store up to one-week-worth of events. Both OM series units incorporate non-volatile memory capable of storing all events until power/cellular are restored at which time the events would be reported and posted including date and time of day.
4a.51	Equipment	All straps utilized to attach equipment to an offender shall be designed so that if an offender cuts, severs or otherwise compromises the integrity of the strap an alert is generated.	**Sentinel exceeds this requirement.** The OM series unit detects three (3) tamper types including 1) strap tamper, 2) device tamper and 3) device removal. Within approximately one (1) second of a tamper attempt, the device will communicate and send a unique alert to the SenTrak web interface. **The OM series device will automatically and instantly communicate to the SenTrak software when a participant attempts to remove or tamper with the strap.** The SenTrak system then immediately sends the alert to the appropriate agency defined personnel. The elapsed time for a device tamper to be executed and then have a notification via text message and/or voice call is under 45 seconds. The OM series device will send a tamper alert if the participant severs the strap or if the unit loses contact with the back plate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit. The OM series devices offer the most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. **The devices remain in tamper until inspected and are reset through the SenTrak software.** The reduction in excessive tamper events that are a nuisance to officers reduces tamper events to only those that truly warrant investigation and necessitate oversight. If an officer is not near a computer, he or she may call the Sentinel monitoring center to clear any tamper event. For each tamper event, officers can program multiple notifications, such as reminders. **IMPORTANT SENTINEL ADVANTAGE: Automatic reset is an outdated approach commonly used by vendors whose equipment experiences a high volume of false tamper alarms and consequently, by automatically resetting, makes it highly prone for a tamper to be overlooked if the band**

			is re-closed as it will automatically reset. Advanced GPS devices such as the OM series devices have been developed that do not suffer from false tampers, thus the device stays in tamper until evaluated by an officer, then can be reset via the web-based system or via remote data device (such as BlackBerry).
4a.52	Equipment	Straps used to attach the equipment to an offender shall have exterior surfaces made of hypoallergenic materials, and shall be adjustable in length to fit all offenders. All straps designed to attach equipment to an offender shall have the capability to be securely sized to an offender. If straps are pre-sized they shall be immediately available in one-half inch increments or less.	**Sentinel meets this requirement.** The strap and backplate used to attach the OM series are hypoallergenic. The OM series device, backplate and strap are easily sanitized and reusable on multiple participants without the need for replacement. The device is attached to the participant's ankle with an extended length band to accommodate the largest of ankles. The strap's design allows for a secure fit and has multiple holes to assist in finding the proper fit on each person. The strap is adjustable as needed prior to locking the pins in place to allow the participant to stand up and/or walk around to determine the best fit possible.
4a.53	Equipment	GPS devices should be able to utilize additional accessories (such as beacons or similar RF monitoring devices) for enhanced location verification in defined impaired environments while at home.	**Sentinel exceeds this requirement.** The OM400 offers an optional companion beacon, Please note that upon the basis that the OM series units have secondary AFLT cellular triangulation, this optional beacon is NOT commonly needed for primary GPS tracking rather, merely an option for adding indoor RF monitoring and/or to offer landline reporting in the rare occurrence a participant lives in an area without cellular coverage. In addition to the use of GPS, all OM series devices have secondary location technologies including **Assisted GPS and Advanced Forward Link Trilateration (AFLT) to determine par** **IMPORTANT SENTINEL ADVANTA** secondary location technologies including OM Series AFLT Diagram 

some impaired environments such as the participant's home, car floorboards, buildings, buses and/or other weak satellite locations. Unique to the OM series devices is the utilization of **Advanced Forward Link Trilateration (AFLT)**, GPS and Assisted GPS to locate the unit. This enhanced dual-monitoring feature allows reliable location tracking from a single device even in impaired environments. AFLT triangulates utilizing ambient longitude and latitude data advertised in the environment. Sprint and Qualcomm employ this technology to locate cell phone users who dial 911. In ideal conditions, the OM series acquires a GPS signal within 60 seconds and provides virtually continuous real-time location data of monitored participants. When the device registers no GPS signal, the **OM series devices' AFLT will provide the agency unmatched confidence that the device is reliably monitoring the participant's location.** Other vendors' older technologies that use standalone GPS cannot do this and will not track participants in areas where GPS is impaired (for example: inside buildings) but OM series devices will.

PLEASE NOTE: The AFLT functionally remains active for all OM series monitoring levels at all times. Some competing vendors will claim their device incorporates AFLT but in fact do not include this feature in their pricing and supply devices to agencies with this feature tuned-off.

In the following sample screen, the participant is being tracked while inside a large building commonly not possible for GPS alone however, the AFLT may enable tracking in such impaired locations.

AFTL Tracking Inside a Large Building

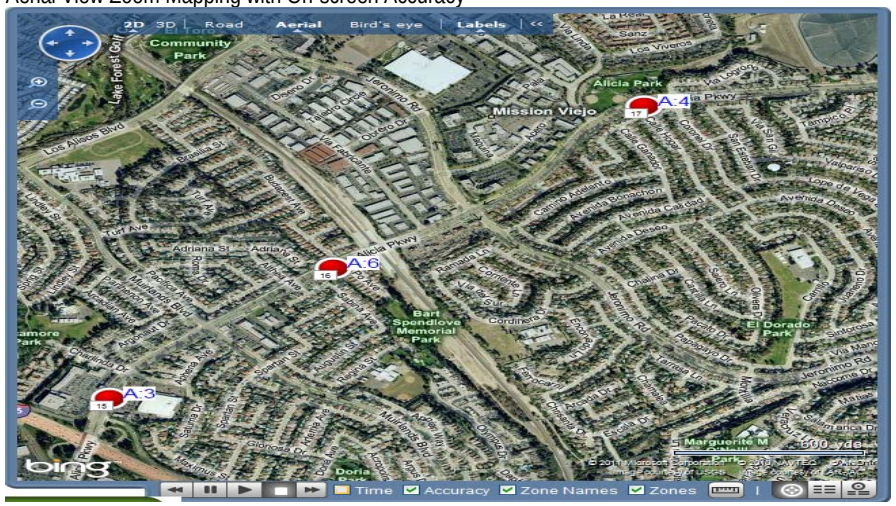
All GPS manufacturers utilize the same government satellites. Therefore,

all GPS leading systems are comparable in accuracy terms as the accuracy is directly related to the number of satellites that are being received by the GPS receiver; the more satellites the more accurate the positioning fix. The accuracy could roughly be broken out as shown in the following chart:

Number of Satellites	Degree of Accuracy
1 - 2 satellites	No fix can be established
3 - 4 satellites	30 meter accuracy
4 - 6 satellites	10 - 30 meter accuracy
7 - 9 satellites	3 - 10 meter accuracy
10 or more	Better than 3 meter accuracy

Therefore GPS accuracy can vary with any GPS manufacturer based on the satellite reception at any given point **therefore it is important for officer's to be able to promptly determine the accuracy of any tracking point in order to determine the basis for compliance and/or potential violation.**

IMPORTANT SENTINEL ADVANTAGE: The mapping screen shown to the right has a unique on-screen accuracy toolbar identified at the bottom of the screen with a check box for "Accuracy." Clicking this box adds a comment next to each tracking point referencing "A:XX." This references the accuracy at each point whereby the "XX" is the number of meters in deviance. (Example on following page: The point with "A:8" is within approximately 8 meters (roughly 26 feet) of accuracy.)

			Aerial View Zoom Mapping with On-screen Accuracy  **Additionally, the proposed software features the proprietary "Precision Engine" software that automatically maximizes the accuracy of the multiple location technologies (GPS, Assisted GPS and/or AFLT) into one (1) point, generating one (1) of the most accurate GPS points available.** **IMPORTANT SENTINEL ADVANTAGE:** In an effort to compete, other vendors offering devices exclusively on the GSM network(s) (incompatible with Sprint's AFLT) have begun to promote cleverly worded alternatives such as "TBT – Tower Based Tracking", "Layered Location Capability", and "Advanced Secondary Location Tracking (ASLT)" These alternatives do not truly provide enhanced tracking but rather only provide secondary shaded areas indicative of the location of cellular towers that the GPS device is communicating that could be miles away and not indicative of the area in which the actual tracking device is located. These alternatives result in officers having to compare the primary tracking points to these secondary shaded areas and then having to make a best guess to determine the location accurately. These factors are widely known by the most experienced GPS users and can be verified through the reference checks as part of this RFP evaluation.
4a.54	Equipment	The GPS device should also have the ability to download location and alert	**Sentinel meets this requirement.** The OM400 offers an optional companion beacon with optional capability to download location and alert information via

		information via landline in areas without adequate cellular coverage.	landline in areas without adequate cellular coverage. Please note that upon the basis that the OM series units have secondary AFLT cellular triangulation, this optional beacon is NOT commonly needed for primary GPS tracking rather, merely an option for adding indoor radio frequency monitoring and/or to offer landline reporting in the rare occurrence a participant lives in an area without cellular coverage.
4b.0	**SECTION D Equipment Requirements – multi-piece tracking system**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
4b.1	Equipment	Vendor is bidding the following multi-piece GPS tracking system and the accessories identified in the Price Worksheets. In the multi-piece configuration, there are two separate units. One unit is body-attached and the other unit is body-worn. The responses to these specifications are for this equipment. **Device attached to the body:** Mfg.: _____ Brand/Model: _____ **Device worn on the body:** Mfg.: _____ Brand/Model: _____	**Sentinel meets this requirement.** **Device attached to the body:** Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II Transceiver **Device worn on the body:** Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II GPS Tracking Device **Device installed in the home:** Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II Home Monitoring Unit
4b.2	Equipment	The Vendor shall provide, at their own expense, all systems and equipment (software and hardware) required for the service delivery, regardless of the actual number of systems including but not limited to:	**Sentinel meets this requirement.** Sentinel Offender Services will provide, at its own expense, all of the systems and equipment required for the service delivery, regardless of the actual number of systems. As a leading provider of monitoring services throughout the industry, Sentinel has spent more than 20 years servicing offender monitoring programs nationwide. Sentinel operates some of the largest programs in the country exceeding 1,000 offenders while simultaneously supporting agencies using less than five (5) active devices. Sentinel is prepared to continue providing service to agencies of differing sizes and is pleased to present the **TrakMate II – Multi Piece GPS Tracking System** solution to the Western States Contracting Alliance and its participating agencies. The TrakMate II is a complete solution for flexible GPS offender tracking. The TrakMate II GPS Tracking device is equipped with GPS tracking technology and

			an embedded receiver capable of receiving signals from the transceiver worn on the offender's ankle. The TrakMate II uses CDMA cellular networks to communicate with the monitoring center, and provides active, passive and intermediate (hybrid) tracking. The TrakMate II acquires a new position point every minute and communicates that information to the monitoring centers as frequently as every five (5) minutes or as infrequently as every 10 minutes depending on agency preference while in active tracking mode. **Both the frequency of acquisition and the frequency of communication to the monitoring center are adjustable upon request. Some of the unique benefits of the TrakMate II solution are as follows:** ▪ **Expanded GPS Acquisition Capability:** TrakMate II GPS Tracking Unit communicates with the Global Positioning System satellite constellation operated by the United States Federal Government. **TrakMate II uses 12 parallel channel receivers to continuously track 12 satellites. This is the best acquisition capability in the GPS industry and far exceeds industry standards.** ▪ **Redundant Monitoring Coverage:** Sentinel takes a unique approach to providing a GPS tracking solution to criminal justice agencies. Sentinel designed the TrakMate II GPS system to provide **"Redundant GPS over RF"** location monitoring of an offender by utilizing **the GPS tracking device to track the offender's movements while away from the residence, while the home monitoring unit ensures compliance with residential curfew requirements by using standard radio frequency communication.** ▪ **Voice Communication:** Sentinel also pioneered the **Direct Voice Communication** feature, which allows agency officers to call and speak with an offender at any time day or night by placing a call directly to the TrakMate II GPS Tracking Device. **The TrakMate II's direct voice communication feature is vastly superior to other multiple-piece GPS equipment models that only offer paging or one-way text-messaging capabilities, if any at all.** ▪ **Light-Emitting Diode (LED) Display:** In order to simplify and facilitate the confirmation of a properly-installed ankle device, Sentinel's transceiver is manufactured with a built-in LED on the front panel of the transceiver case. This LED eliminates any lingering doubt about installation, which sometimes occurs when installing other ankle-worn bracelet models where the installer can not immediately verify if the ankle-worn transceiver is actually functional. ▪ **Ease of Installation:** Sentinel's transceiver has been designed for ease

			of installation and/or removal and durability. **Sentinel's ankle-worn transceiver is only three (3) pieces – the transceiver, backplate and strap,** while other vendors' transmitters can have more than 10 individual pieces making a mere installation laborious due to the multiple steps required. ▪ **Extended Battery Life and Storage:** The TrakMate II can provide real time tracking data for more than 24 hours without recharging the battery and in the event an offender would enter an area with no cellular coverage and the TrakMate II will store up to one month's worth of tracking data for download when the participant returns to cellular coverage or docks his/her phone in the HMU. Another benefit of the ankle-worn transmitter is that the extended battery lifespan allows Sentinel's units to remain in service longer than other models without the need for concern about repeated battery replacement. ▪ **Tamper Alert and Reset:** For security purposes, the strap is designed so that the transceiver can detect if the strap has been cut or severed by the participant. The TrakMate II ankle-worn transceiver incorporates an automatic tamper reset. This feature allows the transceiver to reset itself in the event that the device has received an impact yet there was not a tamper with the device. ▪ **Motion Detection:** Sentinel's TrakMate II transceiver also has an internal accelerometer that will **report a "No Motion" alarm** if the transceiver does not move for several hours. This provides a redundant tamper feature with a purpose similar to that of the proximity tamper seen in other electronic monitoring transmitters. In the extremely unlikely event that a participant removes the transceiver without tampering the ankle strap, the "No Motion" alarm will be triggered alerting authorized personnel.
4b.3	Equipment	a. A system with a database to monitor offender activity;	**Sentinel meets this requirement.** Today, Sentinel provides service to more than 60,000 offenders utilizing some of the most advanced monitoring and case management software systems in the industry. SenTrak, Sentinel's proprietary software, is utilized to perform all GPS tracking services. **Using this system, all agencies and authorized personnel, have real-time, online access to participant monitoring activity and information.** Sentinel internally developed the software and provides all scheduled maintenance to ensure that the system remains in optimal operational status at all times. Authorized personnel using SenTrak can view and print monitoring activity reports at any time. SenTrak also has the ability to notify the designated person immediately upon

			receipt of any tracking information to the monitoring center. Simultaneously, SenTrak can distribute alerts to multiple locations/persons. The ability to parse data and customize the automated process makes the minimum processing time mere seconds. For maximum functionality when utilizing the TrakMate II GPS tracking solution, SenTrak is designed in an SQL (Sequential Query Language) format that allows for user-specific queries to pull data from **any field** in the database. Sentinel can generate reports providing details on any specific item or list of items on the participant population that would be required by the agency. Reports can be prepared to provide demographic queries based on name, age, address, height, weight, etc., as well as court-related data including court information, officer information, case number(s), conviction charges, program compliance and others. This comprehensive data can then be used to provide detailed statistics for the entire participant population.
4b.4	Equipment	b. All monitoring units (transmitter, receiver/dialer and other related equipment) to communicate location data to the Vendor's system;	**Sentinel exceeds this requirement.** The TrakMate II GPS Tracking Device employs the largest cellular footprint in the nation to communicate its location data to the monitoring system utilizing CDMA technology and the wireless services of both Verizon and Sprint. The TrakMate II is also capable of transmitting location data utilizing through the HMU and its landline telephone service connection whenever cellular communication is unavailable. This ensures that all location data is able to be transmitted to the monitoring system and thus accessible by authorized agency personnel. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel takes a unique approach to providing a GPS tracking solution to criminal justice agencies. Sentinel designed the TrakMate II GPS system to provide **"Redundant GPS over RF"** location monitoring of an offender by utilizing both the portable TrakMate II GPS Tracking Device along with the TrakMate II Home Monitoring Unit (HMU). The TrakMate transceiver worn by the offender com PS Tracking Device and the HMU providing 24-hour, in e the offender is at his and/or her residence, the TrakM

			built in docking station on the HMU and the monitoring is done through radio frequency tethering of the transceiver to the HMU, eliminating all "drift" problems. **This functional design format allows the GPS tracking device to track the offender's movements while away from the residence, while the home monitoring unit ensures compliance with residential curfew requirements by using standard radio frequency communication.** This combination of portable GPS tracking and residential radio frequency monitoring creates a redundant system design which guarantees highly dependable, continuous monitoring and tracking 24 hours a day, seven (7) days a week of each program participant.
4b.5	Equipment	c. All software and hardware required to access the Internet, with the exception of Agency personal computers; and	**Sentinel meets this requirement.** Sentinel's proprietary software, SenTrak, is a web-based system that provides a user-friendly interface for offender enrollment, mapping, scheduling, zone creation, and communication. Sentinel's internal Information Technology (IT) department developed, owns and operates the SenTrak system, providing in-house maintenance expertise as well as total control over the database, data field queries, reports and overall operations. Authorized personnel have the capability to use SenTrak software to enroll new offenders, establish zones, modify schedules, and view the latest activity and violation information. Authorized personnel using SenTrak can view and modify offender curfew schedules and view and print monitoring activity reports. SenTrak also allows agency personnel to make notes about offender-generated alerts. All these features are available in real-time, any time, and anywhere via a totally web-based system. SenTrak is accessible over the Internet by authorized personnel, through secure connections and password-protected interfaces. **Sentinel customers do not need to purchase or download any custom hardware or software.** Upon program enrollment, Sentinel assigns security passwords and unique login names to SenTrak users. **As a web-based system, SenTrak does not require any special software, plug-ins, or hardware for access by designated personnel.** Sentinel's IT staff has installed all of the necessary physical and technical security measures (i.e., SSL certificates, network firewalls, anti-virus software, access control equipment, and closed-circuit television) to ensure that unauthorized users and hackers do not have access to SenTrak or the monitoring center. **IMPORTANT SENTINEL ADVANTAGAE:** As part of the SenTrak software functionality, officers will have remote access to SenTrak via handheld PDAs,

			laptops, Blackberries, Droids, ect. The device allows officers to connect to the SenTrak host system wirelessly and will display offender locations and caseload status through high quality digital maps that are clearly displayed on the screen. Also, the officers can call the offenders directly from the wireless device in order to more easily utilize the TrakMate II Voice Feature. When accessed through a handheld device, the SenTrak software allows one touch dialing to the offender's TrakMate II GPS tracking device. As the solution allows direct access into the SenTrak offender tracking system, one (1) of the features Sentinel provides is the ability to display the participant's image and residential information. Any digital picture of the participant can be uploaded into the SenTrak system and directly into his and/or file. This allows officers to be able to report to a residence and if not personally aware of the participant's appearance, they can quickly retrieve his image on their handheld units and search for the participant quickly. This eliminates the need to have officers carry voluminous files or journals with booking pictures as the software can provide all participant information within seconds, directly from the system.
4b.6	Equipment	d. All labor, materials, equipment, cellular wireless service costs and consumables necessary to perform GPS tracking services on an as-needed basis.	**Sentinel meets this requirement.** Sentinel understands the importance of providing the necessary personnel, materials, equipment, cellular wireless service costs, and consumables associated with performing GPS tracking services and will do so if awarded.
4b.7	Equipment	All equipment and systems furnished shall be standard products supplied by the Vendor, shall be in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.	**Sentinel meets this requirement.** Sentinel is the designer and owner for all of the TrakMate II multi-piece GPS tracking system devices. TrakMate II multi-piece GPS tracking system is a standard product supplied by Sentinel. Each component of the multi-piece system is manufactured in Southern California specifically for electronic monitoring of offenders within the criminal justice system. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. **Sentinel employs a Quality Assurance Plan that includes a Final Quality Checklist to the ensure that all initial and new equipment shipments leave the warehouse in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the offender in normal intended use.**
4b.8	Equipment	The Vendor shall provide only equipment that meets the highest levels of ruggedness, durability and performance	**Sentinel exceeds this requirement.** Sentinel's TrakMate II multi-piece GPS tracking solution incorporates the TrakMate II Transceiver as the body-attached, one-piece device and the TrakMate II GPS Tracking Device as the body-worn

<table>
<tr>
<td></td>
<td></td>
<td>available, when considering the following: operating temperature, stored temperature range, temperature cycling, shock and vibration, water resistance or waterproofing, operating humidity range, stored humidity range and tamper resistance.</td>
<td>cellular communication device. Sentinel also incorporates the TrakMate II Home Monitoring Unit in order to not only serve as the docking station to recharge the TrakMate II GPS Tracking Device but to also provide compliance with residential curfew requirements through redundant RF over GPS monitoring ensuring the elimination of “drift” typical of some GPS tracking devices while indoors.

Each of these devices have been in service on thousands of offenders nationwide. Each has been designed to meet the highest standards in equipment durability and performance. All of Sentinel’s equipment has been manufactured and designed to pass rigorous testing for temperature, shock, water resistance and tamper capabilities. For example, the TrakMate II GPS tracking solution equipment has been designed to meet or exceed the following standards:
<table>
<tr><th>Feature</th><th>TrakMate II Durability Standard</th></tr>
<tr><td>Stored/Operating Temperature</td><td>32° F to 158° F (0° C - 70° C) +/- 10%</td></tr>
<tr><td>Temperature Cycling</td><td>No restriction within stored /operating temperature limits</td></tr>
<tr><td>Shock</td><td>ISTA - CATEGORY 1A SHOCK FREE FALL</td></tr>
<tr><td>Vibration</td><td>ISTA CATEGORY - 1A 2.5HZ ASTM D 999-01 Method A1</td></tr>
<tr><td>Water</td><td>Water Resistant Case</td></tr>
<tr><td>Operating Humidity Range</td><td>10-90% Relative Humidity Non-condensing</td></tr>
<tr><td>Stored Humidity Range</td><td>10-90% Relative Humidity Non-condensing</td></tr>
<tr><td>Tamper Resistance</td><td>Case Tamper, Strap Tamper, Accelerometer</td></tr>
</table>
</td>
</tr>
<tr>
<td>4b.9</td>
<td>Equipment</td>
<td>The tracking system shall include one-piece body-attached device and a body-worn cellular communication device. Performance information and product literature may be included in Vendor’s proposal response.</td>
<td>Sentinel meets this requirement. Sentinel’s TrakMate II multi-piece GPS tracking solution incorporates the TrakMate II Transceiver as the body-attached, one-piece device and the TrakMate II GPS Tracking Device as the body-worn cellular communication device. Sentinel also incorporates the TrakMate II Home Monitoring Unit in order to not only serve as the docking station to recharge the TrakMate II GPS Tracking Device but to also provide compliance with residential curfew requirements through redundant RF over GPS monitoring ensuring the elimination of “drift” typical of some GPS tracking devices while indoors. The TrakMate II body-attached transceiver has the following</td>
</tr>
</table>

			features: **Light-Emitting Diode (LED) Display:** In order to simplify and facilitate the confirmation of a properly-installed ankle device, the TrakMate II transceiver is manufactured with a built-in LED on the front panel of the transceiver case. When the installation is performed, the LED will flash green for several seconds notifying the installer that the unit has been properly installed and that it is functional. This LED eliminates any lingering doubt about installation, which sometimes occurs when installing other ankle-worn bracelet models where the installer can not immediately verify if the ankle-worn transmitter is actually functional. **Ease of Installation:** The TrakMate II transceiver has been designed for ease of installation / removal and durability featuring **only three (3) pieces – the transceiver, backplate, and strap,** while other vendors' transmitters can have more than ten (10) individual pieces making a mere installation laborious due to the multiple steps required. The TrakMate II transceiver's snap and lock installation requires no tools as the strap is secured between the backplate and transceiver and locked in place when the unit is snapped on the offender's ankle. The strap is specially designed so that it can only be installed in one (1) direction, eliminating issues with other vendor equipment straps that can actually be incorrectly installed and jeopardize proper operation of the device. For the comfort of the wearer, the strap consists of hypoallergenic materials. For security purposes, the strap is designed so that the transceiver unit can detect if the strap has been cut or severed by the offender. If so, the transceiver will immediately generate a tamper alert. Additionally, the TrakMate II ankle-worn transceiver does not pose a safety risk or hazard to offenders or any other persons. **Extended Battery Life:** The TrakMate II can provide real time tracking data for more than 24 hours without recharging the battery and in the event an offender would enter an area with no cellular coverage and the TrakMate II will store up to one month's worth of tracking data for download when the participant returns to cellular coverage or docks his/her phone in the HMU. Another benefit of the ankle-worn transceiver is that the extended battery lifespan allows the unit to remain in service longer than other models without the need for concern about repeated battery replacement. The TrakMate II ankle-worn transceiver battery is designed to last for a minimum of 12 months before needing to be replaced.

			Sealed Transceiver Case: In order to ensure that it is waterproof, the battery has been completely enclosed and sealed in the TrakMate II transceiver casing. This eliminates problems present in other models with removable batteries where moisture can enter the inner components through the battery insertion area, thereby jeopardizing operation and reliability. The seal on the TrakMate II transceiver has been designed to operate under normal atmospheric conditions and temperatures. It is water-proof and shock-resistant and allows a participant to conduct all normal daily activities, including showering, without affecting the transmitter's operation. **Automatic Tamper Reset:** The TrakMate II transceiver incorporates an automatic tamper reset. This feature allows the transceiver to reset itself in the event that the device has received an impact yet there was not a tamper with the device. This eliminates the need to call the participant into the office or to have authorized personnel perform a field-check. **Motion Detection:** Sentinel's TrakMate II transceiver also has an internal accelerometer that will **report a "No Motion" alarm** if the transceiver does not move for several hours. This provides a redundant tamper feature with a purpose similar to that of the proximity tamper seen in other electronic monitoring transmitters. In the extremely unlikely event that a participant removes the transceiver without tampering the ankle strap, the "No Motion" alarm will be triggered alerting authorized personnel. The **TrakMate II GPS Tracking Device** uses CDMA cellular networks for its telecommunications capabilities in an inconspicuous cellular phone to be worn or carried by the program participant that is discrete, lightweight, tamper-resistant, and made of abuse-resistant material. Our TrakMate II GPS Tracking Device does not pose any safety hazards to the offender or anyone in the residence. The unit will function reliably under normal environmental and atmospheric conditions and incorporates the following features: **Voice Communication:** Sentinel pioneered the **Direct Voice Communication** feature, which allows agency officers to call and speak with an offender at any time day or night by placing a call directly to the TrakMate II GPS Tracking Device. The TrakMate II GPS Tracking Device's telephone number is secure and not provided to participants, and participants are aware that they must answer all calls received since only an agency officer or a monitoring center operator would attempt to make contact via the TrakMate II calling feature. The

			TrakMate II does not allow offenders to make outgoing phone calls. In addition to providing state-of-the-art GPS tracking and mapping, this direct communication feature provides an additional layer of supervision, as participants are aware that agency officers can call them at any time to speak with them. **The TrakMate II's direct voice communication feature is vastly superior to other multiple-piece GPS equipment models that only offer paging or one-way text-messaging capabilities, if any at all.** **Expanded GPS Acquisition Capability:** Sentinel's TrakMate II GPS Tracking Device, through its built-in 12-channel satellite receiver, is able to receive location data from up to 12 individual satellites. This high-capacity reception allows for a more accurate determination of the participant's location to within a 50-foot radius, under optimal conditions. Other GPS tracking devices have smaller receiver capabilities that may affect the accuracy of individual point identification due to the inability to connect with the required number of satellites to successfully configure a tracking point. The **TrakMate II Home Monitoring Unit (HMU)** is Sentinel's docking station and charging base for the TrakMate II GPS Tracking Device and has the following unique features. **Redundant Coverage:** Sentinel takes a unique approach to providing a GPS tracking solution to criminal justice agencies. Sentinel designed the TrakMate II GPS system to provide **"Redundant GPS over RF"** location monitoring of an offender by utilizing both the portable TrakMate II GPS Tracking Device along with the TrakMate II Home Monitoring Unit (HMU). This functional design format allows the GPS Tracking Device to track the offender's movements while away from the residence, while the HMU ensures compliance with residential curfew requirements. The TrakMate transceiver worn by the offender communicates with both the GPS Tracking Device and the HMU providing 24-hour, intensive supervision. While the offender is at his and/or her residence, the TrakMate II is recharged in the built in docking station on the HMU and the monitoring is done through radio frequency tethering of the transceiver to the HMU, eliminating all "drift" problems. **This functional design format allows the GPS tracking device to track the offender's movements while away from the residence, while the home monitoring unit ensures compliance with residential curfew requirements by using standard radio frequency communication.** This combination of portable GPS tracking and residential radio frequency monitoring creates a redundant system design which guarantees

			highly dependable, continuous monitoring and tracking 24 hours a day, seven (7) days a week of each program participant. **Landline Communications:** In addition to performing as a traditional home curfew unit, the HMU also downloads and sends GPS tracking points and compliance information stored in the TrakMate II GPS Tracking Devices to the monitoring center over traditional landline telephone service. The TrakMate II HMU uses a standard RJ-11 telephone jack that allows for the immediate and automatic transmission of offender status, e.g., curfew compliance and tamper information, through the residential telephone line to the monitoring center. The TrakMate II HMU utilizes a toll-free number so there is no cost to the participant.
4b.10	Equipment	The Vendor shall provide equipment that meets market safety standards and presents no health or safety hazards to staff and/or offenders.	**Sentinel exceeds this requirement.** All of the TrakMate II GPS tracking solution equipment meets industry safety standards and does not pose any health or safety hazards to staff or offenders. Sentinel is the designer and owner of the TrakMate II GPS tracking solution manufactured in Southern California. All of Sentinel's TrakMate II equipment, e.g., the TrakMate II GPS Tracking Device, the TrakMate II Transceiver, and the TrakMate II HMU is created according to Sentinel's own original designs and manufactured according to specification. Some equipment subcomponents are outsourced to manufacturing partners who comply with ISO 9001 quality standards. **IMPORTANT SENTINEL ADVANTANGE:** In addition to the proposed devices being manufactured in ISO certified facilities, Sentinel is ISO 9001:2008 certified as an electronic monitoring provider and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations and monitoring center including agency/departmental specific operational procedures.
4b.11	Equipment	The device identified by the Vendor above shall be the latest proven reliable technology and meet the requirements specified in Items 1.2 and 1.3 above.	**Sentinel exceeds this requirement.** Sentinel is proposing its latest generation, most advanced multi-piece TrakMate II GPS tracking system and SenTrak software, which have been in continuous use for more than four (4) years in agencies nationwide and has been installed and in use on significantly more than 500 offenders with Sentinel acting as the prime contractor for equipment and services. Sentinel has provided a list containing the State, Federal or local government agencies with the associated volumes for the TrakMate II GPS tracking solution in the Appendix D: Bidder Information and Profile section of this proposal and additionally in the response to Item 1.2 as required.
4b.12	Equipment	The one-piece body-attached device shall not have any sharp edges and shall be	**Sentinel meets this requirement.** Sentinel's TrakMate II Transceiver will be used as the one-piece body-attached device for the TrakMate II multi-piece GPS

		designed so not to cause excessive chafing or bruising.	tracking solution. The transceiver weighs 2.7 ounces fully assembled and is designed with rounded edges so as not to cause any discomfort, chafing or bruising to the participant while being worn. The strap and backplate used to attach the transceiver are hypoallergenic.
4b.13	Equipment	The body-worn device shall use Global Position Satellites and the cellular telephone network to track and report the location(s) of offenders both at home and in the community, regardless of location. Passive, Hybrid, and Active tracking shall be provided by the GPS tracking system.	**Sentinel exceeds this requirement.** The TrakMate II GPS Tracking Device communicates with the Global Positioning System's satellite constellation operated by the United States Federal Government. The TrakMate II utilizes a built-in 12 channel GPS chip to continuously receive location data from up to 12 individual satellites 24 hours a day, seven (7) days a week– **the best acquisition capability in the GPS industry**. This high-capacity reception allows for a more accurate determination of the offender's location to within a 50-foot radius, under optimal conditions. Sentinel designed the TrakMate II to utilize the largest cellular footprint in the country - CDMA technology and the wireless services of both Verizon and Sprint. The TrakMate II is also designed to "roam" on any available CDMA service provider in the area. **IMPORTANT SENTINEL ADVANTANGE:** Sentinel takes a unique approach to providing a GPS tracking solution to criminal justice agencies. Sentinel designed the TrakMate II GPS system to provide **"Redundant GPS over RF"** location monitoring of an offender by utilizing both the portable TrakMate II GPS Tracking Device along with the TrakMate II Home Monitoring Unit (HMU). This functional design format allows the GPS Tracking Device to track the offender's movements while away from the residence, while the HMU ensures compliance with residential curfew requirements. The TrakMate transceiver worn by the offender communicates with both the GPS Tracking Device and the HMU providing 24-hour, intensive supervision. While the offender is at his and/or her residence, the TrakMate II is recharged in the built in docking station on the HMU and the monitoring is done through radio frequency tethering of the transceiver to the HMU, eliminating all "drift" problems. **This functional design format allows the GPS tracking device to track the offender's movements while away from the residence, while the home monitoring unit ensures compliance with residential curfew requirements by using standard radio frequency communication.** This combination of portable GPS tracking and residential radio frequency monitoring creates a redundant system design which guarantees highly dependable, continuous monitoring and tracking 24 hours a day, seven (7) days a week of each program participant.

			IMPORTANT SENTINEL ADVANTANGE: In addition to providing highly accurate home monitoring of the offender, **the use of the TrakMate II HMU eliminates issues found in other GPS systems that do not utilize a home monitoring unit as a part of their multi-piece GPS application.** With other providers, the GPS unit is tasked with all facets of the offender tracking and monitoring, including residential coverage when the offender is required to be at home. In these situations, GPS devices are subject to "satellite drift" issues. This inherent GPS-related issue causes stationary GPS units to generate a displayed variance in the true position or in other words, show point information "drifting" from where the offender is actually located. This may account for erroneous mapping displays showing the offender leaving his/her inclusion zone, thus exiting the residence during the middle of the night since the accuracy of the GPS point diminishes due to the constantly changing movement and visible availability of the satellites in orbit. **Sentinel's TrakMate II GPS Tracking Device provides active, passive and intermediate (or Hybrid) GPS tracking levels to easily adjust with the needs of any program**. **The levels of service are built-in to the software and do not require Sentinel staff or agency staff to "change out" or replace equipment in order to change a participant's level of GPS super**vision. Sentinel's levels of GPS tracking are: **Active GPS:** Using the active level of GPS tracking, authorized personnel can track participants 24 hours a day, seven (7) days a week, acquiring position data once every minute and reporting position data to the software every 15 minutes. In fact, with active tracking the TrakMate II GPS Tracking Device is adjustable to call in as frequently as every five (5) minutes or as infrequently as every 15 minutes depending on agency preference. Active GPS tracking also allows authorized staff (Sentinel and agency) to set **inclusion and exclusion zones** to restrict offenders' movements around the community. Staff may modify the zones as needed at anytime through the SenTrak software. All alarms and violations are processed in near real-time format for near immediate notification by the SenTrak software. In addition to communicating with the monitoring center systems, the TrakMate II allows an officer to call the offender and speak with them directly through our patented communication feature. The phone can be programmed to restrict use by the offender, e.g., the offender can only receive calls from an agency staff member or Sentinel personnel. This direct voice feature is more beneficial and reliable than other products that utilize text

			message-based communications with offenders. **Intermediate/Hybrid GPS:** Sentinel was the first company in this industry to create an intermediate or hybrid level of GPS tracking. By design the TrakMate II GPS Tacking Device will collect a location point once (1) per minute and report to the software every 30 minutes when in a non-alert condition. In fact, with hybrid tracking the TrakMate II GPS Tracking Device is adjustable to call in as frequently as every five (5) minutes or as infrequently as every 30 minutes depending on agency preference. Additionally, equipment and schedule violations are reported immediately to the designated agency personnel based on agency notification protocols. Geographic zones are also available at this tracking level, and zone violations are visible in the software/mapping but not notified in real time. In the hybrid (intermediate) setting, agency personnel may also contact/call and communicate with the participant using the voice communication feature of the TrakMate II GPS Tracking Device. **Passive GPS:** This tracking level is traditionally used for the lower-risk participants. While away from the residence, the TrakMate II system will track and store all participant movements (GPS points). By design the TrakMate II GPS Tacking Device will collect a location point once (1) per minute and report to the software every 12 hours when in a non-alert condition. Passive GPS tracking offers more monitoring information than ordinary radio frequency electronic monitoring and as such, it is the next level in progressive supervision of offenders. Geographic zones can still be used in this level similar to the intermediate tracking service. Equipment tampers and low battery signals are still reported in real time, however location information is available only at predetermined intervals selected by the agency (usually every 12 to 24 hours). As required for this response, Sentinel will default every WSCA customer to a reporting frequency of no less than once every 12 hours which may be shortened at the agency's request.
4b.14	Equipment	Active GPS shall be 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	**Sentinel exceeds this requirement.** In active tracking mode, Sentinel's TrakMate II GPS Tracking Device collects a tracking point or location once every minute. **The tracking points are then reported via the cellular network to the monitoring center system every 15 minutes. In fact, with active tracking the TrakMate II GPS Tracking Device is adjustable to call in as frequently as every five (5) minutes or as infrequently as every 15 minutes depending on agency preference, and therefore can far exceed the requirement of reporting at least every 15 minutes.** When a tamper or zone violation occurs, the violation is immediately reported to the monitoring center

		not evaluated.	system and a violation alert is sent in order for appropriate officer response. Based on agency requirements, all alarms will be processed within the required timeframes and notifications are sent as required to any electronic messaging enabled system (text, email, etc.) or direct officer contact. In addition to communicating with the monitoring center systems, the TrakMate II allows an officer to call the offender and speak with them directly through our patented communication feature. The phone can be programmed to restrict use by the offender, e.g., the offender can only receive calls from an agency staff member or Sentinel personnel. This direct voice feature is more beneficial and reliable than other products that utilize text message-based communications with offenders.
4b.15	Equipment	Passive GPS shall be 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.	**Sentinel meets this requirement.** In Passive tracking mode, Sentinel's TrakMate II GPS Tracking Device collects a tracking point or location point once every minute. Since this tracking level is traditionally used for the lower-risk participants, passive GPS allows only historical/end-of-day/next-day reporting. While away from the residence, the TrakMate II system will track and store all participant movements (GPS points). Geographic zones can still be used in this level, and equipment tampers and low battery signals are still reported in real time; however, location information is available only at predetermined intervals selected by the agency (usually every 12 to 24 hours). **As required for this response, Sentinel will default every WSCA customer to a reporting frequency of no less than once every 12 hours which may be shortened at the agency's request.**
4b.16	Equipment	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.	**Sentinel exceeds this requirement.** Sentinel was the first company in this industry to create an intermediate or hybrid level of GPS tracking. By design the TrakMate II GPS Tacking Device will collect a location point once (1) per minute and report to the software every 30 minutes when in a non-alert condition. In fact, with hybrid tracking the TrakMate II GPS Tracking Device is adjustable to call in as frequently as every five (5) minutes or as infrequently as every 30 minutes depending on agency preference. If utilized at its most intensive level, hybrid tracking allows authorized personnel to view any participants GPS tracking information to obtain information that is no more than five (5) minutes old through the SenTrak software 24 hours a day. Additionally, equipment and schedule violations are reported immediately to the designated agency personnel based on agency notification protocols. Geographic zones are also available at this tracking level, and zone violations are visible in the software/mapping but not notified in real time. In the hybrid (intermediate) setting, agency personnel may also contact/call and communicate with the participant using the voice communication feature of the TrakMate II GPS Tracking Device.
4b.17	Equipment	Active GPS includes the ability of the	**Sentinel exceeds this requirement.** At no additional cost, though utilizing

		body-worn device to be remotely contacted to force the device to instantly locate and call back with its data immediately. Vendor shall include unlimited instant cellular locates at no additional costs.	**either the active or hybrid GPS levels**, Sentinel's TrakMate II GPS Tracking Device acquires one (1) GPS location point per minute and downloads all acquired points to the monitoring system as frequently as every five (5) minutes. This intensive level of reporting exceeds most active and hybrid reporting levels and far exceeds the requirement for this RFP. Due to this intensive reporting capability, near real-time information is available for all active and hybrid GPS tracking participants on an on-going basis virtually eliminating the need for on-demand location capabilities as the average "ping" or "on-demand" location request takes anywhere from two to three (2 – 3) minutes to complete and additional time to report through the cellular networks to the monitoring system.
4b.18	Equipment	The system must be capable of utilizing unlimited alternative location tracking using the cellular network in the absence of GPS at no additional costs.	**Sentinel exceeds this requirement.** Sentinel surpassed all other vendors in the GPS arena with the design and release of the TrakMate II product. The TrakMate II GPS Tracking Device utilizes the latest and most reliable 12-channel receiver GPS chip in the industry. Where some companies may only utilize a 4- to 6-channel chipset, Sentinel uses a 12-channel approach and incorporates only the strongest received signals. The accuracy of the points provided by the TrakMate II GPS Tracking Device are enhanced through this 12-channel GPS chip. This ability to filter down the satellites to the strongest message, allows the TrakMate II equipment to generate position locations that are often times spot on, or within 20 feet of the actual location. It is not uncommon for the TrakMate II GPS Tracking Device to track a participant not only into a parking lot, but actually down to the parking space he and/or she has chosen. Additionally, the TrakMate II GPS Tracking Device is Assisted GPS capable and designed to utilize secondary cellular tracking capabilities for even greater accuracy when necessary. Through the utilization of cellular networks and the most advanced GPS chip set available, the TrakMate II even tracks indoors and provides latitude and longitude data through most residential facilities. Sentinel has incorporated the latest chip set, Assisted GPS capability and cellular technology available to ensure that every opportunity for a successful location is provided. More importantly, Sentinel has designed the TrakMate II GPS Tracking Device to allow for a new GPS chip should a better more sophisticated chip ever be produced and is designed for enhancements as new cellular based tracking technologies become available. This in house design allows Sentinel to continually provide upgrades as market conditions and technologies change.
4b.19	Equipment	Describe how the web based system reflects the alternative tracking verses GPS tracking and how the location	**Sentinel meets this requirement.** Sentinel's SenTrak software displays all of the necessary features to ensure quality supervision including GPS location information, speed, direction, and event (i.e. schedule, zone, tamper, etc.)

		indicators on the map differentiate between the two.	detection analysis. SenTrak's mapping software also allows the visual display of both GPS points and assisted locations using different color points. When a multi-piece GPS tracking location point is provided, it is displayed in **"Red"**. When the software displays an alternative tracking point for multi-piece GPS tracking participants, the information is presented using a **"Blue"** colored point. This multi color approach makes reviewing location information easy for the supervising officer to determine the origination of each point.
4b.20	Equipment	The system shall have the capacity to convert a body-worn device between active and passive mode without removal from the Offender or requiring a change of equipment.	**Sentinel meets this requirement.** The TrakMate II GPS Tracking Device provides active, passive, and intermediate (hybrid) GPS tracking to easily adjust with the needs of any program. The levels of service are built-in to the software and **do not** require "change out" or replacement of equipment in order to change an offender's level of GPS supervision.
4b.21	Equipment	Both the body-attached and the body-worn devices shall be small, light, and not restrictive and the body-attached device can be attached to the offender in a manner that will not impede normal activities or work. It shall attach securely around the ankle of the offender.	**Sentinel meets this requirement.** Sentinel's body-attached device, the TrakMate II Transceiver, weighs a mere 1.48 ounces fully assembled with the backplate and strap. It measures 2.48 x 1.68 x 1.18 inches. It is light weight and one of the smallest transceivers in the industry so as not to restrict or impede an offender during normal activities or work. Special tools are **not** necessary for the installation of the TrakMate II Transceiver. The unique design consists of only three (3) pieces; the transceiver unit, the ankle strap and the back plate. T he TrakMate II Transceiver is securely attached to the offender's ankle with an adjustable strap. Installation is an easy step-by-step procedure that requires very little training and minimal experience. A typical installation for the ankle-worn device takes less than five (5) minutes. Sentinel's body-worn device, the TrakMate II GPS Tracking Device weighs 6.5 ounces and measures 5.1 x 1.9 x 1.2 inches. It is constructed with a glass fiber re-enforced cover thus keeping the unit light yet durable. The TrakMate II GPS Tracking Device will not restrict the activities of the offender while carrying the device.
4b.22	Equipment	The equipment used shall not pose a safety hazard nor unduly restrict offenders' activities.	**Sentinel meets this requirement.** Both the TrakMate II GPS Tracking Device and the TrakMate II Transceiver are designed so that they do not pose a safety hazard or unduly restrict the offender's activities. These devices have been used on thousands of offenders nationwide and Sentinel has never had a report of the unit having posed a health or safety hazard.
4b.23	Equipment	All equipment assigned to the offender shall be manufactured to allow for repeated proper sanitization. The Vendor shall provide instructions to sanitize the	**Sentinel meets this requirement.** All equipment associated with the TrakMate II GPS tracking solution is designed and manufactured in a manner that allows for ease of cleaning and sanitation. Each device is manufactured for use on multiple offenders and therefore designed to withstand normal and repeated

		equipment, including recommended cleaning agents and methods.	cleaning practices. During the training process, authorized personnel will be provided with written instructions and trained on the recommended cleaning methods and products best suited for thorough sanitation.
4b.24	Equipment	The body-attached device components are quickly removable by a trained officer and are not easily removable except by an officer with the correct equipment.	**Sentinel meets this requirement.** Sentinel's transmitter has been designed for ease of removal and durability. The snap and lock design of the TrakMate II Transceiver allows for quick and easy removal by a trained officer. Using a pair of standard #170 shears, provided at no cost to the agency, the officer will separate the transceiver from the disposable backplate and strap. On each end of the transceiver are two (2) channels with two (2) small holes at the bottom of each. By placing the points of the shears into the holes then cutting the plastic and twisting the shears after making the cut, the officer releases the locking mechanism of the backplate from the transceiver. This step is repeated on the opposite end of the unit as well in order to release the transceiver from the backplate and strap. The transceiver will now pull away from the backplate in order to dispose of the backplate as well as the strap. Removal of the transceiver by a trained officer takes only seconds to complete. While the design of the TrakMate II Transceiver allows for easy officer removal, the transceiver is designed with a **secure locking mechanism that cannot be unlocked or removed without leaving "tell-tale" signs of the tamper efforts of the offender**. Once the transceiver is properly installed, it cannot be removed unless the strap is cut or the transceiver itself is damaged. Any attempt to cut the strap or damage the transceiver case (e.g., remove the backplate) will generate a tamper alarm. Any determined attempt to tamper with or remove the device will also be obvious upon visual inspection. If an offender tries to remove a properly installed transceiver by slipping it off the ankle, the transceiver will recognize the unnatural strain on the strap and again the transceiver will report a tamper alarm. Additionally, Sentinel's TrakMate II Transceiver also has an internal accelerometer that will **report a "No Motion" alarm** if the transceiver does not move for several hours. This provides a redundant tamper feature with a purpose similar to that of the proximity tamper seen in other electronic monitoring transmitters. In the extremely unlikely event that a participant removes the transceiver without tampering the ankle strap, the "No Motion" alarm will be triggered alerting authorized personnel.
4b.25	Equipment	All communications to and from the system's devices shall be encrypted.	**Sentinel meets this requirement.** Sentinel's TrakMate II multi-piece GPS tracking solution operates using a non-commercially available frequency range that is not interfered with by sheriff, police, correctional, or commercial communications equipment. Sentinel has used these products on thousands of offenders and has not experienced any interference from components using

			commercial frequencies. In addition, the communication between the TrakMate II Transceiver and the TrakMate II GPS Tracking Device as well as the TrakMate II HMU is sent via an encoded, secure radio frequency signal over multiple bandwidths once every 17 to 22 seconds. Additionally, all communications to and from the TrakMate II GPS tracking solution and the residential home monitoring unit are delivered to the monitoring center through encrypted, proprietary scripts that ensure data integrity.
4b.26	Equipment	The body-attached device shall be supplied with an installation kit containing all necessary equipment to install, activate or deactivate the device.	**Sentinel exceeds this requirement.** Sentinel's TrakMate II Transceiver has been designed for ease of installation / removal and durability. **Sentinel's ankle-worn transmitter is only three (3) pieces – the transceiver, backplate and strap,** while other vendors' transmitters can have more than 10 individual pieces making a mere installation laborious due to the multiple steps required. TrakMate II Transceiver's snap-and-lock installation requires **no tools** as the strap is secured between the backplate and transceiver and locked in place when the unit is snapped on the participant's ankle. The strap is specially designed so that it can only be installed in one (1) direction, eliminating issues with other vendor equipment straps that can actually be incorrectly installed and jeopardize proper operation of the transceiver. Sentinel will provide the installation kits that contain extra backplates and straps for ease of officer installation and inventory control.
4b.27	Equipment	The body-worn device shall be simple to use and have easy to understand instructions.	**Sentinel meets this requirement.** The TrakMate II GPS Tracking Device is equipped with the latest, field-tested firmware and is shipped to each customer site with most configurations pre-loaded on the device. Upon completion of enrollment via Sentinel's secure web-based software platform, SenTrak, agency personnel complete the configuration process via a short over-the-air data transfer wherein the TrakMate II Transceiver ID and the GPS tracking intervals are downloaded to the TrakMate II Tracking Device and a GPS position is acquired. A complete instruction guide will be provided to agency personnel for training and implementation. Installation takes less than five (5) minutes once the officer has entered his and/or her desired reporting frequency and monitoring level.
4b.28	Equipment	Both devices shall be permanently marked with the model/serial identification numbers and will withstand exposure to common cleaning products. The Vendor will replace either device without charge if the tracking number is not legible.	**Sentinel meets this requirement.** Sentinel utilizes a bar code system on each and every product manufactured and shipped from its warehouse. At the time of manufacturing, each unit is given a unique serial number that is permanently inscribed on the outside of the unit. Because the serial number is inscribed on the unit, it can withstand exposure to common cleaning products as well as daily bathing by the offender. In addition, this serial number is placed on a bar code sticker that is securely attached to the unit. Utilizing the bar code and bar code

			scanner, Sentinel is able to track equipment as it moves between customer sites and Sentinel's warehouse location. Sentinel understands the need to replace any device if the serial number is no longer legible and agrees to comply with this requirement at no additional charge.
4b.29	Equipment	The system shall be capable of tracking an offender twenty-four (24) hours a day, 7 days a week and shall be able to confirm the date, time and location of the tracking event.	**Sentinel meets this requirement.** The TrakMate II multi-piece GPS tracking solution is specifically designed for the criminal justice industry and provides reliable, continuous 24 hour a day, seven (7) day a week, 365 day a year offender tracking via GPS technology. Through the TrakMate II GPS tracking solution, Sentinel offers intensive tracking of offenders at one point per minute at all levels of tracking and records and stores each point with the date, time and location of the event for use in monitoring a participant's compliance with court orders and terms/conditions of probation.
4b.30	Equipment	System devices and all additional equipment shall not be available as an open market item if this could compromise the security of the system.	**Sentinel meets this requirement.** Sentinel's TrakMate II multi-piece GPS tracking solution features non-commercially available devices in order to maintain the security of the system and the reliability of the participant's monitoring. Sentinel is the designer and owner of the TrakMate II multi-piece GPS tracking solution, which is manufactured in Southern California. All of the TrakMate II multi-piece GPS tracking equipment is created according to Sentinel's original designs and manufactured according to specification.
4b.31	Equipment	The strap and circuitry shall enable the system to immediately notify the Monitoring Center of any tamper attempt or removal of the body-attached device from the offenders' ankle.	**Sentinel exceeds this requirement.** The TrakMate II Transceiver is "tamper-alert" and therefore designed to detect report tamper attempts in a variety of ways. Once the transceiver and strap are properly installed, the transceiver cannot be removed unless the strap is cut or the transceiver itself is damaged. Based on the location of the participant, the tamper alarm will be detected and **immediately reported** by either the TrakMate II Home Monitoring Unit (if at home) or by the TrakMate II GPS Tracking Device (if out in the community. Any attempt to cut the strap or damage the TrakMate II Transceiver case (e.g., remove the backplate) will generate a tamper alarm. Any determined attempt to tamper with or remove the device will be obvious upon visual inspection as well. If an offender tries to remove a properly installed transceiver by slipping it off the ankle, the transceiver will recognize the unnatural strain on the strap and the transceiver will report a tamper alarm. **IMPORTANT SENTINEL ADVANTAGE:** The TrakMate II Transceivers also have an internal accelerometer, which will report a "No Motion" alarm if the transceiver does not move for several hours. In the extremely unlikely event that a participant were able to remove the transceiver without severing the ankle strap, the "No Motion" alarm provides a redundant tamper feature with a purpose

			similar to that described for the "proximity tamper" seen in other electronic monitoring transmitters. Since it is virtually impossible for a live person to remain absolutely motionless for several hours, even while sleeping, a "No Motion" alarm would indicate that a participant may have successfully removed the transceiver without activating another type of tamper alarm.
4b.32	Equipment	The system shall acquire GPS within 5 minutes when placed in an outdoor environment.	**Sentinel exceeds this requirement.** Sentinel's TrakMate II GPS Tracking Device is able to collect a location/position from a "cold start" (acquisition of GPS signal after device activation or battery depletion) in less than one (1) minute or a "warm start" (when coming out of the docking station) in 38 seconds on average. These acquisition times far exceed the requirement of "within 5 minutes" thus demonstrating the superior performance of the TrakMate II multi-piece GPS tracking solution.
4b.33	Equipment	The battery for the body-attached device shall hold a single charge for a minimum period of sixteen (16) hours while performing one minute GPS acquisition and downloading data to the Database System at least once every 15 minutes.	**Sentinel exceeds this requirement.** Sentinel's TrakMate II multi-piece GPS tracking solution is comprised of the TrakMate II Transceiver (body-attached device), the TrakMate II GPS Tracking Device (body-worn device) and the TrakMate II Home Monitoring Unit for dual RF over GPS residential home monitoring. The transceiver has a minimum battery life, while in service, of 12 months. The transceiver is tethered to the TrakMate II GPS Tracking Device in order to create the multi-piece tracking system. The TrakMate II GPS Tracking Device, the body-worn device, demonstrates a battery life in excess of 20 hours from a single charge at the most intensive reporting level available. In other words, the TrakMate II GPS Tracking Device has the ability to provide a 20 hour battery life while tracking data at a collection rate of one (1) location point every minute and while downloading all information to the monitoring center every as frequently as every five (5) minutes. This five (5) minute download interval far exceeds the requirement of transmitting at least once every 15 minutes and battery life will increase with reduced call in frequency thus demonstrating the superior performance of the TrakMate II multi-piece GPS tracking solution.
4b.34	Equipment	The system devices shall be shock-resistant.	**Sentinel exceeds this requirement.** Both the TrakMate II GPS Tracking Device and the TrakMate II Transceiver are ISTA shock-resistant (Category 1A Shock Free Fall) and ISTA vibration-resistant (Category 1A 2.5HS ASTMD 999-01 Method Al).
4b.35	Equipment	The battery for the body-attached device shall 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	**Sentinel exceeds this requirement.** Sentinel's body-attached device, the TrakMate II Transceiver, is designed and manufactured with the battery encased within the unit. This protects the battery from environmental factors that might otherwise reduce the life of the battery. The transceivers battery has a shelf life of at least two (2) years. When in service, it is designed to last for a minimum of

		less. The battery for the body worn device shall be able to re-charge the battery from a dead battery status to maximum capacity (100% charge) in five (5) hours or less.	12 months without needing to charge the device and before needing replacement. This extended battery life is a benefit not seen in many other models that need repeated battery replacement or charging. Sentinel's body-worn device, the TrakMate II GPS Tracking Device can be fully recharged from a completely dead battery with a two (2) hour charge cycle far exceeding the (5) five hour requirement. The TrakMate II GPS Tracking Device demonstrates a battery life exceeding 20 hours from a single charge duration of two (2) hours. This is due to the presence of its dual lithium-ion batteries enclosed within the ruggedized ABS casing. This charging structure ensures the TrakMate II GPS Tracking Device's ability to provide tracking data at a collection rate of one (1) location/point every minute while downloading all information to the monitoring center every five (5) minutes or less frequently depending on agency preference.
4b.36	Equipment	The body-attached device shall have a guaranteed life cycle of not less than twelve (12) months. Each device shall be replaced at specific intervals to avoid device failures due to loss of battery power.	**Sentinel exceeds this requirement.** Sentinel's body-attached device, the TrakMate II Transceiver, is designed and manufactured with the battery encased within the unit. This protects the battery from environmental factors that might otherwise reduce the life of the battery. The transceivers battery has a shelf life of at least two (2) years. When in service, it is designed to last for a minimum of 12 months without needing to charge the device and before needing replacement. This extended battery life is a benefit not seen in many other models that need repeated battery replacement or charging. Sentinel understands the importance of ensuring that all agencies utilizing the TrakMate II Transceiver have the ability to replace the devices at specified intervals in order to avoid failures due to a loss of battery power. Therefore, each transceiver is tracked through Sentinel warehouse and Asset Management software to ensure replacement occurs prior to battery failure. It is also important to note that each transceiver has a low battery signal that indicates well in advance (5 days) of a potential battery issue thus avoiding interruption in the monitoring service.
4b.37	Equipment	System devices shall 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. However, hand held device may be charged using a unit that doubles as home RF monitoring unit.	**Sentinel meets this requirement.** Sentinel's TrakMate II multi-piece GPS tracking system can be used with the TrakMate II HMU. **The TrakMate II HMU** not only has the ability to monitor the presence or absence of the body-worn device, the TrakMate II Transceiver, but it also **serves as the docking station and recharging base for the body-attached device, the TrakMate II GPS Tracking Device.** The TrakMate II HMU uses a standard AC wall adapter with a latching connector in order to supply power to the HMU. The HMU then utilizes this power to charge the TrakMate II GPS Tracking Device.

			The TrakMate II GPS Tracking Device can also be supplied with its own standard six (6) foot charging cord in order for the offender to recharge the device while away from his and/or her residence. A secondary car charger can also accompany the TrakMate II GPS Tracking Device in the event that the offender would need the ability to recharge the unit while traveling in a vehicle.
4b.38	Equipment	The body-worn device shall have internal diagnostics that can determine if it is operating properly and the ability to relay the information to the Vendor's Monitoring Center.	**Sentinel meets this requirement.** The TrakMate II GPS Tracking Device communicates with the monitoring center over the Verizon mobile broadband network as the primary wireless provider. The TrakMate II GPS Tracking Device performs an internal analysis of its functionality and then reports to the monitoring center on its regular schedule as defined by the level of monitoring assigned to the offender, i.e. active, hybrid or passive. Each time the TrakMate II GPS Tracking Device communicates with the monitoring center, it will also report the location of the device, the battery status of the device and whether the device has been tampered. In the event of an equipment failure both the TrakMate II GPS Tracking Device and associated SenTrak software are designed to "read" equipment functionality and report proper operability. In addition to the internal diagnostics performed by the unit itself, the SenTrak software is constantly requiring communication and thus the lack of those scheduled contacts is reported immediately in accordance with agency established notification guidelines.
4b.39	Equipment	System devices shall be designed to prevent tracing or duplication of the signal by other electronic devices or equipment.	**Sentinel meets this requirement.** Sentinel is the designer and owner of the TrakMate II GPS tracking solution manufactured in Southern California. All of Sentinel's TrakMate II equipment, e.g., the TrakMate II GPS Tracking Device, the TrakMate II Transceiver, and the TrakMate II HMU is created according to Sentinel's own original designs and manufactured according to specification. Some equipment subcomponents are outsourced to manufacturing partners who comply with ISO 9001 quality standards. **IMPORTANT SENTINEL ADVANTANGE:** In addition to the proposed devices being manufactured in ISO certified facilities, Sentinel is ISO 9001:2008 certified as an electronic monitoring provider and maintains **CONFIDENTIAL** ISO conforming Standard Operating Procedures for **every aspect** of its monitoring operations and monitoring center including agency/departmental specific operational procedures. Sentinel's TrakMate II multi-piece GPS tracking solution operates using a non-commercially available frequency range that is not interfered with by sheriff, police, correctional, or commercial communications equipment. Sentinel has

			used these products on thousands of offenders and has not experienced any interference or duplication/tracing from components using commercial frequencies. In addition, the communication between the TrakMate II Transceiver and the TrakMate II GPS Tracking Device as well as the TrakMate II HMU is sent via an encoded, secure radio frequency signal over multiple bandwidths once every 17 to 22 seconds thus **disallowing** the duplication of the signal by other commercially available products/devices.
4b.40	Equipment	The body-worn device and software system should be capable of storing up to 99 zones so that zone violations can be immediately reported regardless of the call in frequency.	**Sentinel exceeds this requirement.** Through Sentinel's web-based software platform, SenTrak, authorized personnel are able to create, edit and delete exclusion and inclusion zones. SenTrak allows multiple exclusion and inclusion zones per client and numerous schedules per client, including permanent and temporary schedules that can be associated with zones. **There is no maximum number of inclusion or exclusion zones per offender that can be stored in SenTrak. Additionally, the TrakMate II GPS Tracking Device will store up to 100 zones on the device thus exceeding this requirement.** SenTrak supports overlay of offender movement points onto satellite images, street maps and hybrid maps (satellite imagery overlaid with street maps). SenTrak is also configured to support construction of polygon -shaped zones. SenTrak visually differentiates zones with color-coding, as follows: Inclusion Zone = **Green**; Exclusion Zone = **Red.** Sentinel designed SenTrak to allow easy access to zone-setting parameters. Once an offender is selected for a zone assignment, authorized personnel will simply enter the address of the desired zone location and the range perimeter of the zone. Authorized personnel will select if it is to be an exclusion or inclusion zone and then name the zone for later ease of identification. Once the zone has been established, it can be modified any time. As a service feature to customers, this data entry for geographic zones can also be completed remotely by through Sentinel monitoring center personnel. Through SenTrak, authorized users can create multiple zones to cover larger areas or create travel corridors when required. Sentinel work with each agency on a case-by-case basis to create customized zone templates when needed. Zone templates can also be created where a pre-determined amount of zones are automatically applied to specific offenders or population groups. SenTrak records and reports an offender's entry to and exit from an inclusion as well as an exclusion zone and can immediately report this information utilizing the TrakMate II GPS tracking solution regardless of call in frequency.
4b.41	Equipment	The body-worn device shall communicate to the Vendor's Software	**Sentinel exceeds this requirement.** Sentinel has designed the TrakMate II GPS Tracking Device with the largest cellular footprint in the country. The TrakMate

		System by common cellular carrier, with the option of a secondary cellular carrier (list cellular networks proposed).	II GPS Tracking Device unit utilizes CDMA technology and the wireless services of both **Verizon and Sprint**, two (2) of the largest carriers in the country. Moreover, Sentinel has designed the TrakMate II GPS Tracking Device to **"Roam" on any CDMA available service provider** which has lead to increased coverage capabilities nationwide.
4b.42	Equipment	The body-attached device shall be waterproof, and have been independently tested against the effects of continuous immersion in water. The body-worn device shall be water resistant.	**Sentinel meets this requirement.** In order to ensure waterproof capability, Sentinel's body-attached device, the TrakMate II Transceiver, has the battery enclosed directly inside the transceiver casing. This eliminates problems with removable batteries found in other transmitters, where moisture can enter the inner components through the battery insertion area thereby compromising the overall functionality of the device. The TrakMate II Transceiver has undergone extensive testing to ensure its waterproof casing is able to withstand the rigors associated with submersion not only in bathing situations but also in swimming and hot tub scenarios. This independent testing of the transceiver resulted in showing that the unit can withstand being submerged to a depth of 150 feet. This testing was performed in a scuba diving setting thus allowing Sentinel to also test the effects associated with submersion in a saltwater environment. The successful conclusions derived from this testing have allowed Sentinel to determine the continued reliability of the TrakMate II Transceiver under repeated immersion in water. Sentinel's body-worn device, the TrakMate II GPS Tracking Device, is a fully functioning cellular telephone. Its high impact ABS construction in conjunction with its glass fiber reinforced cover make the TrakMate II not only rugged and durable but also splash proof and water resistant.
4b.43	Equipment	The system may be able to detect and record an alert feature to signal the offender by audible tone or other reliable method. Describe your available features.	**Sentinel exceeds this requirement.** Sentinel prides itself in developing innovative products designed to enhance the monitoring of offenders within the criminal justice arena. With this strategy in mind, Sentinel designed the TrakMate II GPS Tracking Device with features allowing not only communication with the offender but also with features designed to alert the offender to potential issues. The TrakMate II GPS Tracking Device contains a display screen that allows the offender to see the battery life of the unit at all times. This indicator is displayed as a percentage of remaining battery life. When the battery reaches a threshold of 40 percent, the TrakMate II GPS Tracking Device will notify the offender that a low battery situation has begun. The TrakMate II GPS Tracking Device will sound an audible alert as well as begin to vibrate indicating to the offender that

			the battery is depleting and that he and/or she should recharge the unit. The offender can then also visually observe the percentage of remaining battery life of the unit as well as see the "Low Battery" indicator on the screen. At this time designated agency personnel will also receive notification of the "Low Battery" if so desired. The unit will follow the same protocols when the battery life drops to 20 percent again indicating that the offender should recharge the unit and display this information on the screen. Again designated agency personnel can receive immediate notification of the second "Low Battery" alert if so desired. Another unique feature associated with the TrakMate II GPS Tracking Device is its ability to notify the offender if they move too far away from the unit. If the offender inadvertently sets their GPS unit down on a table and walks away from it, the TrakMate II GPS Tracking Device will begin sounding an audible tone directing the offender back to the unit. This tone will sound for two (2) minutes or until the offender returns to the range of the unit. This feature assists the offender in "remembering" to remain within a few feet of the unit at all times. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel also pioneered the **Direct Voice Communication** feature, which allows agency officers to call and speak with an offender at any time day or night by placing a call directly to the TrakMate II GPS Tracking Device. The TrakMate II GPS Tracking Device's telephone number is secure and not provided to participants, and participants are aware that they must answer all calls received since only an agency officer or a monitoring center operator would attempt to make contact via the TrakMate II calling feature. The TrakMate II does not allow offenders to make outgoing phone calls. In addition to providing state-of-the-art GPS tracking and mapping, this direct communication feature provides an additional layer of supervision, as participants are aware that agency officers can call them at any time to speak with them. **The TrakMate II's direct voice communication feature is vastly superior to other multiple-piece GPS equipment models that only offer paging or one-way text-messaging capabilities, if any at all.**
4b.44	Equipment	The system shall be able to detect and record an alert feature with immediate tamper notification.	**Sentinel exceeds this requirement.** The TrakMate II transceiver is designed to report tamper attempts in a variety of ways. Once the transceiver is properly installed, the transceiver cannot be removed unless the strap is cut or the transceiver itself is damaged. Based on the location of the offender, the alarm will be received by the monitoring center systems and immediately reported by either the Home Monitoring Unit or by the TrakMate II GPS unit. Sentinel's TrakMate II Transceiver is designed to report tamper attempts in a

			variety of ways. Once the transceiver is properly installed, the transceiver cannot be removed unless the strap is cut or the transceiver itself is damaged. Based on the location of the participant, the alarm will be received and reported by either the TrakMate II HMU or by the TrakMate II GPS Tracking Device. Any attempt to cut or sever the strap, remove the transceiver, or damage the transceiver case (e.g., remove the backplate) or otherwise compromise the integrity of the strap will generate a tamper alarm. Any determined attempt to tamper with or remove the device will be obvious upon visual inspection as well. **IMPORTANT SENTINEL ADVANTAGE:** The TrakMate II Transceivers also have an internal accelerometer, which will report a "No Motion" alarm if the transceiver does not move for several hours. In the extremely unlikely event that a participant were able to remove the transceiver without severing the ankle strap, the "No Motion" alarm provides a redundant tamper feature with a purpose similar to that described for the "proximity tamper" seen in other electronic monitoring transmitters. Since it is virtually impossible for a live person to remain absolutely motionless for several hours, even while sleeping, a "No Motion" alarm would indicate that a participant may have successfully removed the transceiver without activating another type of tamper alarm. The TrakMate II GPS Tracking Device is also designed with anti-tamper detection capabilities. The unit itself will register and generate a tamper alert if the offender attempts to disassemble/compromise the unit's exterior case. The unit is also designed to perform regularly scheduled check-in calls to the monitoring software to ensure proper operation of the device. If the offender damages the unit and the unit does not report in as required, the SenTrak software system will automatically generate an alarm reporting the GPS device's failure to check-in. Sentinel staff will then immediately investigate the situation to determine the TrakMate II GPS Tracking Device's current status. Additionally, the TrakMate II HMU's are equipped with multiple anti-tamper features as well. All HMU cases are sealed to prevent unauthorized access by an offender. Any attempts to compromise the case will automatically generate and send a tamper alert that will be immediately processed by Sentinel's monitoring center personnel.
4b.45	Equipment	The system shall be able to detect and record an alert feature with immediate alert notification for inclusion and/or exclusion zone violations.	Sentinel meets this requirement. At the time of program enrollment, authorized users enter daily curfew schedules and/or inclusion and exclusion zones for each offender. These are the time limits and locations within which the offender must comply to avoid non-compliance. Each exit from, and entry to, the residence or

			zone (inclusion or exclusion) is reported by the TrakMate II GPS tracking solution to the web-based software platform, SenTrak. SenTrak will then immediately send an alert notification per agency notification procedures. Any discrepancies of the event time or location with the permitted time or location will generate a violation that is immediately processed. This activity verification is continuously performed by SenTrak, which thereby ensures the monitoring of the offender population at all times. Using SenTrak, authorized personnel are able to create, edit, and delete exclusion and inclusion zones for participants being tracked via the TrakMate II GPS tracking solution. These zones are used to control a participant's movements throughout the community. SenTrak allows for an unlimited amount of exclusion and inclusion zones per client. For participants with challenging zones, SenTrak is also configured to support construction of polygon-shaped or non-traditional zones. SenTrak visually differentiates zones with color-coding, as follows: Inclusion Zone = **Green**; Exclusion Zone = **Red.** As a benefit for the programs Sentinel monitors, authorized users can also create **template zones** that can be used across a certain population as needed. This allows agency personnel to designate certain sites across an entire region that can be applied to an entire population. For example, for a sex offender population, agencies can establish pre-determined exclusion zones around schools, playgrounds, or related areas to keep entire program populations away from these "hot zones" without having to re-create the same zones on a continual basis. This type of zone set-up can be used for pedophile, sex offender, and other high-risk participant populations. **IMPORTANT SENTINEL ADVANTAGE:** Google Maps® provides automatic updates to the SenTrak mapping software providing the latest in maps and upgrades at all times. Sentinel does not maintain maps within the SenTrak mapping software, unlike some vendors who must download regular updates to their mapping software– a very time consuming process. SenTrak tracks all location points and overlays the points on the most recent Google Map available at the time of the tracking.
4b.46	Equipment	The system shall be able to detect and report and alert feature with immediate alert notification for loss of communication violations.	**Sentinel meets this requirement.** The TrakMate II multi-piece GPS tracking system has been designed to detect and report loss of communication with both the TrakMate II GPS Tracking Device and the TrakMate II HMU. The TrakMate II GPS Tracking Device and the TrakMate II HMU both generate regularly scheduled "check-in" calls to the monitoring center. These calls are designed to

			ensure continued communication and proper functioning of each device. If either device fails to make its required "check-in" call, the SenTrak software system will automatically generate an immediate alert indicating that there has been a loss of communication with the particular device. This notification can be sent to designated personnel per agency-approved protocols and procedures. Please note: Sentinel is able to differentiate between the loss of GPS coverage and the loss of cellular coverage. This flexibility allows Sentinel customers more options as it relates to establishing notification procedures and enforcement protocols.
4b.47	Equipment	System devices shall be able to detect and record an alert feature with immediate alert notification for a low battery.	**Sentinel meets this requirement.** Sentinel's TrakMate II multi-piece GPS tracking system allows for immediate detection and notification of low battery alerts from all three (3) devices; the TrakMate II Transceiver, the TrakMate II GPS Tracking Device and the TrakMate II HMU. The **TrakMate II Transceivers** extended battery lifespan allows the units to remain in service longer than other models without the need for concern about repeated battery replacement. The transceiver battery is designed to last for a minimum of twelve (12) months before needing to be replaced. When the battery does reach a "Low" threshold, indicating approximately five (5) or more days of battery life still remains, the SenTrak monitoring software will automatically send immediate notification to designated agency personnel. The **TrakMate II GPS Tracking Device** contains a display screen that allows the offender to see the battery life of the unit at all times. This indicator is displayed as a percentage of remaining battery life. When the battery reaches a threshold of 40 percent, the TrakMate II GPS Tracking Device will notify the offender that a low battery situation has begun. The TrakMate II GPS Tracking Device will sound an audible alert as well as begin to vibrate indicating to the offender that the battery is depleting and that he and/or she should recharge the unit. The offender can then also visually observe the percentage of remaining battery life of the unit as well as see the "Low Battery" indicator on the screen. At this time designated agency personnel will also receive notification of the "Low Battery" if so desired. The unit will follow the same protocols when the battery life drops to 20 percent again indicating that the offender should recharge the unit and display this information on the screen. Again designated agency personnel can receive immediate notification of the second "Low Battery" alert if so desired. Lastly, the **TrakMate II HMU**, which serves as the docking station/recharging base for the TrakMate II GPS Tracking Device and for curfew compliance while

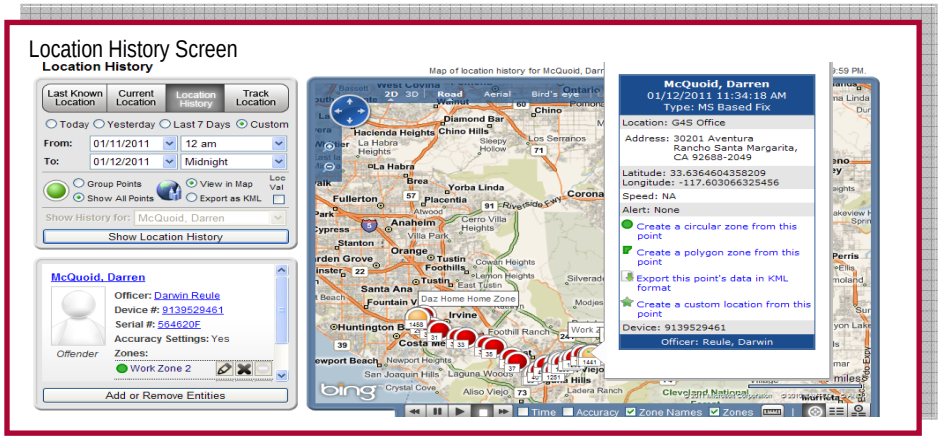
			the offender is at his and/or her residence, is equipped with the **longest-lasting backup battery in the industry providing more than fifty (50+) hours of reserve power,** the occurrence of a "Low Battery" alert is minimized significantly. The TrakMate II HMU can also notify departmental personnel when a "Low Battery" status is reached indicating approximately four (4) hours of battery life remain, assuming no reconnection of residential power.
4b.48	Equipment	The system may be able to detect and record an alert feature with-alert notification to detect potential masking of the device's ability to receive GPS signals.	**Sentinel meets this requirement.** Should a participant successfully shield the TrakMate II GPS Tracking Device in any way, both the incoming GPS signal and the outgoing cellular signal will be blocked and the agency will receive a continued combination "No GPS" – "Late To Test" alert. In these circumstances, Sentinel and/or the agency can contact the participant to inform them that the device is being shielded and walk them through the process to un-shield the device. Through the SenTrak software, Sentinel can differentiate between the inability to communicate via cellular tower and the absence of GPS signals.
4b.49	Equipment	As an optional feature, identify and describe any offender acknowledgement feature located on any system device.	**Sentinel exceeds this requirement.** Sentinel prides itself in developing innovative products designed to enhance the monitoring of offenders within the criminal justice arena. With this strategy in mind, Sentinel has designed the TrakMate II GPS Tracking Device with features allowing not only communication with the offender but also with features designed to alert the offender to potential issues. The TrakMate II GPS Tracking Device contains a display screen that allows the offender to see the battery life of the unit at all times. This indicator is displayed as a percentage of remaining battery life. When the battery reaches a threshold of 40 percent, the TrakMate II GPS Tracking Device will notify the offender that a low battery situation has begun. The TrakMate II will sound an audible alert as well as begin to vibrate indicating to the offender that the battery is depleting and that he and/or she should recharge the unit. The offender can then also visually observe the percentage of remaining battery life on the screen of the unit. The screen will also indicate "Low Battery" as well. The TrakMate II GPS Tracking Device will follow the same protocols when the battery life drops to 20 percent again indicating that the offender should recharge the unit. Another unique feature associated with the TrakMate II GPS Tracking Device is its ability to notify the offender if they move too far away from the unit. If the offender inadvertently sets their GPS unit down on a table and walks away from it, the TrakMate II GPS Tracking Device will begin sounding an audible tone directing the offender back to the unit. This tone will sound for two (2) minutes

			or until the offender returns to the range of the unit. This feature assists the offender in "remembering" to remain within a few feet of the unit at all times. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel also pioneered the **Direct Voice Communication** feature, which allows agency officers to call and speak with an offender at any time day or night by placing a call directly to the TrakMate II GPS Tracking Device. The TrakMate II GPS Tracking Device's telephone number is secure and not provided to participants, and participants are aware that they must answer all calls received since only an agency officer or a monitoring center operator would attempt to make contact via the TrakMate II calling feature. The TrakMate II does not allow offenders to make outgoing phone calls. In addition to providing state-of-the-art GPS tracking and mapping, this direct communication feature provides an additional layer of supervision, as participants are aware that agency officers can call them at any time to speak with them. **The TrakMate II's direct voice communication feature is vastly superior to other multiple-piece GPS equipment models that only offer paging or one-way text-messaging capabilities, if any at all.**
4b.50	Equipment	The body-worn device should incorporate non-volatile memory capable of storing at least 24 hours worth of events (with date and time of occurrence) at times when the cellular service or and electrical power may become unavailable. Non-volatile memory will retain unreported events and report them once power/cellular services have been restored, including date & time of occurrence.	**Sentinel exceeds this requirement.** In the event of a loss of cellular service or power, the TrakMate II GPS Tracking Device incorporates non-volatile memory in order to store location data as well as event data. All information is stored within the TrakMate II GPS Tracking Device with the date and time of the location as well as the date and time of any events that occurred. **This non-volatile memory allows the TrakMate II GPS Tracking Device to store over 10,000 tracking points far exceeding the 24 hour requirement.** Once cellular service and/or electrical power is restored to the TrakMate II GPS Tracking Device, the unit will send out all stored information to the monitoring center for processing.
4b.51	Equipment	All straps utilized to attach equipment to an offender shall be designed so that if an offender cuts, severs or otherwise compromises the integrity of the strap an alert is generated.	**Sentinel exceeds this requirement.** Sentinel's TrakMate II Transceiver is designed to report tamper attempts in a variety of ways. Once the transceiver is properly installed, the transceiver cannot be removed unless the strap is cut or the transceiver itself is damaged. Based on the location of the participant, the alarm will be received and reported by either the TrakMate II HMU or by the TrakMate II GPS Tracking Device. Any attempt to cut or sever the strap or otherwise compromise the integrity of the strap will generate a tamper alarm. Any determined attempt to tamper with or remove the device will be obvious upon visual inspection as well. **IMPORTANT SENTINEL ADVANTAGE:** The TrakMate II Transceivers

			also have an internal accelerometer, which will report a "No Motion" alarm if the transceiver does not move for several hours. In the extremely unlikely event that a participant were able to remove the transceiver without severing the ankle strap, the "No Motion" alarm provides a redundant tamper feature with a purpose similar to that described for the "proximity tamper" seen in other electronic monitoring transmitters. Since it is virtually impossible for a live person to remain absolutely motionless for several hours, even while sleeping, a "No Motion" alarm would indicate that a participant may have successfully removed the transceiver without activating another type of tamper alarm.
4b.52	Equipment	Straps used to attach the equipment to an offender shall have exterior surfaces made of hypoallergenic materials, and shall be adjustable in length to fit all offenders. All straps designed to attach equipment to an offender shall have the capability to be securely sized to an offender. If straps are pre-sized they shall be immediately available in one-half inch increments or less.	**Sentinel meets this requirement.** Sentinel's TrakMate II Transceiver utilizes a strap made of a proprietary, hypoallergenic Elastomer designed for the comfort of the wearer. The interior of the strap contains a non-metal conductive material that will not cause injury or harm to the installer or the wearer. The strap is 14 inches in length and is adjustable in one half-inch increments in order to fit any size participant.
4b.53	Equipment	Deleted.	
4b.54	Equipment	The GPS system device should also have the ability to download location and alert information via landline in areas without adequate cellular coverage.	**Sentinel meets this requirement.** In addition to Sentinel's unique approach of providing redundant GPS over RF through the TrakMate II HMU, **the HMU also downloads and sends GPS tracking points and alert information stored in the TrakMate II GPS Tracking Devices to the monitoring center over traditional landline telephone service.** The TrakMate II HMU uses a standard RJ-11 telephone jack that allows for the immediate and automatic transmission of offender status, e.g., curfew compliance, location information and tamper information, through the residential telephone line to the monitoring center. The TrakMate II HMU utilizes a toll-free number so there is no cost to the participant.
5.0	**SECTION E System, Software and Mapping Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
5.1	System, Software and Mapping	The Vendor shall have a secure web based system and provide the agency with secure access.	**Sentinel meets this requirement.** SenTrak is accessible over the Internet by authorized personnel, through secure connections and password-protected interfaces on any internet-enabled device, such as a computer, laptop, and smart phone. **Sentinel customers do not need to purchase or download any custom hardware or software.** Upon program enrollment, Sentinel assigns security passwords and unique login names to **all authorized agency personnel**.

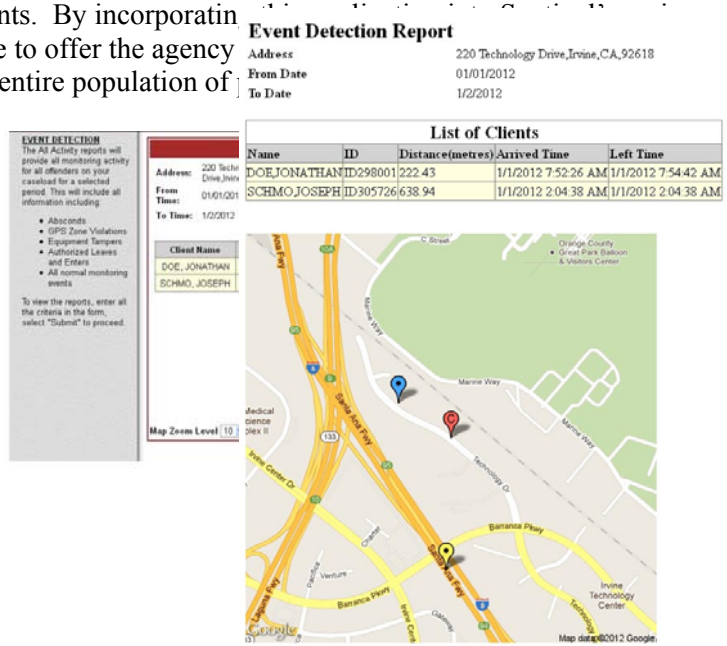
			Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked. The SenTrak software uses leading Internet security features, including 128-bit encryption and Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions, uses HyperText Transfer Protocol (HTTP) and is accessible through a standard high-speed Internet connection. Sentinel's IT staff has installed all of the necessary physical and technical security measures (i.e., SSL certificates, network firewalls, anti-virus software, access control equipment, and closed-circuit television) to ensure that unauthorized users and hackers do not have access to SenTrak or the monitoring center.
5.2	System, Software and Mapping	The Vendor's web site shall not require any software downloads or remote access to the Agency's computers to utilize the system.	**Sentinel meets this requirement.** The SenTrak software application is a secure web-based HTTPS environment application that is easily accessible for authorized users worldwide 24 hours a day, seven (7) days a week, 365 days a year on any internet-enabled device, such as a computer, laptop, and smart phone. **Sentinel customers do not need to purchase or download any custom hardware or software.**
5.3	System, Software and Mapping	The Vendor shall provide a web-based system that is capable of being accessed through a secure (password protected) internet connection from desktop, laptop or remote means by Agency personnel, who have appropriate security clearance and have been provided Vendor-supplied security codes.	**Sentinel meets this requirement.** SenTrak is accessible over the Internet by authorized personnel, through secure connections and password-protected interfaces on any internet-enabled device, such as a computer, laptop, and smart phone. **Sentinel customers do not need to purchase or download any custom hardware or software.** Upon program enrollment, Sentinel assigns security passwords and unique login names to **all authorized agency personnel**. Sentinel has a stringent password policy that ensures that the system is not vulnerable to any brute force type of attack where passwords can easily be cracked.
5.4	System, Software and Mapping	The Vendor's system shall be supported by a database that allows for multiple data fields, subject to final approval by the Agency.	**Sentinel meets this requirement.** The SenTrak system is be supported by an expandable database that allows for multiple data fields, subject to final approval by the agency. Using SenTrak officers can profile new participants. To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's name, agency designated unique alpha-numeric identifier, physical address, serial number of assigned equipment, time zone, assigned officer, and offender photo. In addition to entering the basic requirements, an agency can choose participant demographic information, offers free field fields and allows agencies to request customized fields for additional agency specific participant information. Sentinel is the original developer of SenTrak and Sentinel engineers control the web-based data fields, reports and

			queries, ensuring Sentinel is fully capable of meeting agency data and reporting needs.
5.5	System, Software and Mapping	The Vendor's web-based application shall provide the ability to efficiently stream aerial mapping data and offender tracking points with minimal latency during critical hours of operations and concurrency.	**Sentinel meets this requirement.** The equipment offerings discussed in this proposal are designed specifically for continuous and real-time GPS tracking supported by the proposed web-based software platform to receive, store, and disseminate data generated from the field through multiple communication methods including toll-free telephone, email, and fax. The SenTrak system database has unlimited ability for expansion to ensure efficient streaming of aerial mapping data and offender tracking points with minimal latency during critical hours of operations and concurrency. The SenTrak mapping software providing the latest in maps and upgrades at all times though Bing Maps and Google Maps®. Both Google Maps and Bing Maps have state-of-the-art graphics including aerial mapping capabilities and much more. For example, Bing Maps utilized with the one-piece GPS tracking solution can be view in aerial, road, 2D, 3D and Bird's Eye views and can show state, county, municipality and street names at the discretion of the user. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel does not maintain maps within the SenTrak mapping software, unlike some vendors who must download regular updates to their mapping software– a very time consuming process. SenTrak tracks all location points and overlays the one-piece GPS tracking points on the most recent Bing Map available and the multi-piece GPS tracking points on the most recent Google Map available at the time of the tracking.
5.6	System, Software and Mapping	The Vendor's web-based application shall be accessible twenty four (24) hours per day, 365 days per year while maintaining acceptable processing performance for offender mapping and tracking data.	**Sentinel meets this requirement.** The SenTrak software application is a secure web-based HTTPS environment application that is easily accessible for authorized users worldwide 24 hours a day, seven (7) days a week, 365 days a year on any internet-enabled device, such as a computer, laptop, and smart phone. The SenTrak system database has unlimited ability for expansion to ensure continued acceptable processing performance for offender mapping and tracking data.
5.7	System, Software and Mapping	Any software necessary for Agency interface shall be provided at the expense of the Vendor, with no licensing fee to the Agency.	**Sentinel meets this requirement.** SenTrak is accessible over the Internet by authorized personnel, through secure connections and password-protected interfaces. **Sentinel customers do not need to purchase or download any custom hardware or software.**
5.8	System, Software and Mapping	The Vendor's web-based application shall allow users to access the application over an SSL connection with 128 bit encryption, utilizing Microsoft Explorer	**Sentinel meets this requirement.** The SenTrak software is accessible utilizing Microsoft Internet Explorer 5.0 or higher and uses leading Internet security features, including 128-bit encryption and Secure Sockets Layer (SSL), the same security features employed by top banking and insurance institutions, uses

		web browser version 6 or higher.	HyperText Transfer Protocol (HTTP) and is accessible through a standard high-speed Internet connection. Sentinel's IT staff has installed all of the necessary physical and technical security measures (i.e., SSL certificates, network firewalls, anti-virus software, access control equipment, and closed-circuit television) to ensure that unauthorized users and hackers do not have access to SenTrak or the monitoring center.
5.9	System, Software and Mapping	The Vendor's system shall provide the capability for the Agency to download data and reports from the database, through secured internet access.	**Sentinel exceeds this requirement.** All authorized users have the ability to directly access participant information, to download data and generate reports through SenTrak**.** Additionally, the SenTrak system provides users with real-time access to caseload data, including participant events, violations and daily statuses. SenTrak allows all authorized users with a computer and Internet browser (i.e. home computer, office computer, other) to exchange monitoring and tracking data, such as enrollment, curfew and zone assignment or changes, caseload review, reports and terminations, with the Sentinel monitoring center using secure website access provides alert notifications to its customers for a wide array of violations and events.
5.10	System, Software and Mapping	The Vendor's system shall have the capability to query the database for any/all GPS offenders based on a specified dates times and locations.	**Sentinel meets this requirement.** All authorized users have the capability to query the SenTrak database for any/all GPS offenders based on a specified dates times and locations. For all GPS participants, real-time and all historical participant information can be accessed through the SenTrak software. Please note: Users have the ability to view historical GPS points for specified date ranges. The mapping history will display every point recorded or it can group points for more clarity.  Sentinel's SenTrak web-based monitoring application features a built-in "event

			detection" platform for all multi-piece GPS tracking participants. This Sentinel solution can also provide crime correlation data to check the proximity of any one-piece GPS participant to any specified location(s) at any historical time. (Please note: This feature is described more fully later in this proposal.)
5.11	System, Software and Mapping	The Vendor's system shall provide the capability for the entry of narrative-style notes by Agency personnel and/or the Vendor's monitoring center staff. These notes will be utilized as documentation of steps taken to resolve offender alerts.	**Sentinel meets this requirement.** Authorized users (agency or monitoring center) can enter free-style case notes on a "per participant" or "per event" basis. Once a note has been entered, it cannot be removed from the system. All notes are archived to create a clear audit trail of all participant monitoring activities. All archived participant notes are also available to view through the software. SenTrak also allows agency personnel to make notes about offender-generated alerts. All these features are available in real-time, any time, and anywhere via a totally web-based system.
5.12	System, Software and Mapping	The Vendor's system shall be able to allow configuration of protocols to enable the features that the Agency wants and disable those that it does not want. For example, types of alerts, notifications, zone categories, etc.	**Sentinel meets this requirement.** SenTrak also allows for authorized personnel to determine alarm and notification protocols. Prior to deployment, Sentinel's operations team can meet with department personnel to establish group level alarm and notification protocols. Once these groups, such as "high risk", are established, the department can place individuals within the specific group and receive alarms and notifications as dictated by the pre-determined protocols for that group. The agency can set instantaneous response, end of day notification summary or no notification requirements. Sentinel will work with each Western States Contracting Alliance participating agency to ensure all notifications are customized to meet personnel schedules, set work day hours, off time, etc. to guarantee the appropriate response times to ensure public safety. As the SenTrak monitoring software is an in-house concept and design, SenTrak is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support.** Sentinel will work with each participating agency to enable the features that the agency wants and disable those that it does not want.
5.13	System, Software and Mapping	The Vendor's system shall show the officer in charge of the offender: name, phone numbers, etc if different from the offender's assigned officer ('on call' staff).	**Sentinel exceeds this requirement.** All authorized users including assigned officers or on-duty officers have the ability to view an offender's name, phone numbers, and other demographic information for the purposes of monitoring/tracking offender compliance. Additionally, **alert notifications sent to all officers and/or supervisors will include the offender's name, phone numbers, and other demographic information essential for follow-up**.
5.14	System, Software and Mapping	The Vendor's system shall be able to record the model and serial number.	**Sentinel exceeds this requirement.** The Using SenTrak officers can profile new participant enrollments. To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's name, agency designated unique alpha-numeric identifier, physical address, serial

			number of assigned equipment, time zone, assigned officer, and offender photo. In addition to entering the basic requirements, an agency can choose participant demographic information, offers free field fields and allows agencies to request customized fields for additional agency specific participant information. Sentinel is the original developer of SenTrak and Sentinel engineers control the web-based data fields, reports and queries, ensuring Sentinel is fully capable of meeting agency data and reporting needs.
5.15	System, Software and Mapping	The Vendor's system shall be able to assign to users role-based security levels. These include, but are not limited to, manager, supervisor, and Officer.	**Sentinel meets this requirement.** The SenTrak system provides administrative capability for managing a user's access level. The program administrator controls whether users have subordinate or peer-level access and assigns user names and passwords. Access can be set to a limited level where a user has access only to his or her caseload status or it can be set to a tiered-level, based on hierarchy of users and agency administrators including mangers, supervisors and officers. Typically, only senior level staff are assigned the highest access level, allowing access to all officers and all participant information and statuses. Regardless of the access level assigned, all users have access to the options for viewing, saving and/or printing data and/or reports, ensuring effective and efficient information exchange and report generation.
5.16	System, Software and Mapping	The Vendor's system is able to accept critical event data points and be able to link Offender's to the event on the map.	**Sentinel meets this requirement.** Sentinel's SenTrak web-based monitoring application features a built-in "event detection" platform for all multi-piece GPS tracking participants. By incorporatin portal, we are able to offer the agency participant or the entire population of matter of minutes. **Authorized personnel can enter the date, time and location of any incident and promptly receive a**



			report of all participants who were near the location. The results of the query can also be graphically displayed on an individual map allowing the event and plotted participant information, relative to the query, to be viewed. Authorized personnel are able to perform these searches at any time from any Internet–enabled computer. A "results" table is generated depicting all participants who were within the proximity of the incident. **This map distinguishes the incident location by placing a red star upon the location. Each participant within the specified radius of the incident is identified. This report can be viewed on screen or printed for later review.** **IMPORTANT SENTINEL ADVANTAGE:** All "event detection" participant, geographic, and latitude and longitude data can be exported and provided to multiple law enforcement agencies for cross reference with their own internal and/or proprietary mapping software. This software option is provided at **no cost** to the agency. This Sentinel solution can also provide crime correlation data to check the proximity of any one-piece GPS participant to any specified location(s) at any historical time. The SenTrak software has, through the use of Proximity Report utility to show if a target offender or offenders were in proximity of a particular address or location of a crime. This report can be generated by simply entering an address of interest including a crime incident report address and running the report. These reports will stay within the system until a new address is entered but saved indefinitely for a permanent record through exporting the report to Excel. The Proximity Report shows the name of the offender, the date and time, Latitude, Longitude, Distance to the address, the specific address identified, the offender device ID as well as an active link to view the tracking points via mapping for each participant identified by the query.
5.17	System, Software and Mapping	The Vendor's system shall provide administrative access to website tracking report showing by user: how many log-ins/minutes logged in by month summary detailed reports with date/duration/time stamp per log on.	**Sentinel meets this requirement.** Summary administrative information is available through SenTrak for all participating agencies utilizing one-piece GPS devices. SenTrak will generate a standardized User Activity Report that displays all user activity by user including how many log-ins/minutes logged in by month summary detailed reports with date/duration/time stamp per log on. Currently, SenTrak also will generate a standardized Supervisor Report that shows activity and caseload of agency users. As the SenTrak monitoring software is an in-house concept and design, **Sentinel is not reliant on an outside vendor for new editions or support.** As the SenTrak monitoring software is an in-house concept and design, Sentinel can

<table>
<tr><td></td><td></td><td></td><td>provide customized reports on a per agency-basis. Sentinel catapulted the speed, capacity and capabilities of monitoring software through the development of the SenTrak SQL database system for two-piece monitoring participants. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective.</td></tr>
<tr><td>5.18</td><td>System, Software and Mapping</td><td>The Vendor's system shall enable the Agency to monitor the near real time position for a specific offender's location at any and all times. Offender location data shall be uploaded a minimum of once every 15 minutes while in compliance and immediately uploaded when the offender is in violation status. The system shall provide offender locations upon demand. The system shall also be capable of the following:</td><td>

Sentinel exceeds this requirement. Both the proposed one-piece and multi-piece GPS solutions system enables any participating agency to monitor the near real time position for a specific offender's location at any and all times.

OM series devices are single unit devices that are both the receiver of location information and the transmitter of status and location information. The OM Series, **through its supporting software without removal or changing of equipment,** provides the flexibility an agency needs for controlling the level of supervision each participant receives to meet individual monitoring needs and budget constraints. This level is defined by the type of monitoring assigned in the participant's risk profile. The risk profile not only defines the monitoring intensity, but also allows the agency to change the level, based on a participant's current monitoring status. Risk profiles available include, but are not limited to:

<table>
<tr><th>Risk Profile</th><th>Mode of Operation</th></tr>
<tr><td>Active Monitoring</td><td>Acquires a GPS point every 60 second increments and automatically transmits data every 15 minutes. Tampers are immediately transmitted.</td></tr>
<tr><td>Hybrid Monitoring</td><td>Acquires a GPS point every 60 seconds and automatically transmits data every 30 minutes. Tampers are immediately transmitted.</td></tr>
<tr><td>Passive Monitoring</td><td>Acquires a GPS point every 60 seconds and automatically transmits data every 12 hours. Tampers are immediately transmitted.</td></tr>
</table>

In the event of an alert condition and regardless of the mode of operation, the OM Series will report the alert immediately, further the device will automatically increase its transmission frequency to a one (1) minute GPS point, one (1) minute impaired locate through AFLT and a one (1) minute transmission of monitoring data under alert conditions.

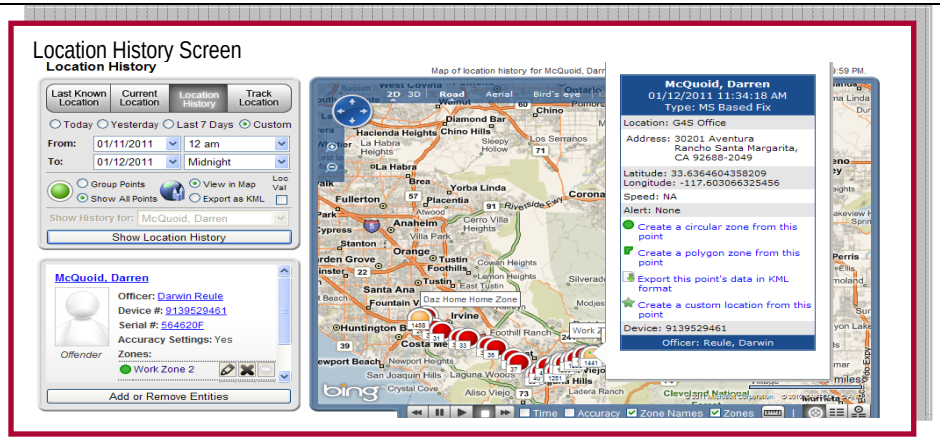
The OM Series also has the capability to change the frequency of monitoring automatically when an exclusion zone has been breached. When an exclusion

</td></tr>
</table>

			zone is breached several things occur. First, an exclusion zone alert is reported to the monitoring software and then sent out immediately as directed by agency to users supervising the participant. Second, the device reverts into "constant tracking" mode. In this mode, the device will use all three (3) location methods (GPS, Assisted GPS and AFLT via cellular tower triangulation) to determine and report locations in real time. It will remain in this mode until the device leaves the exclusion zone or the battery is exhausted. In addition, users can add a buffer zone around an exclusion zone for added safety. Buffer zones may or may not be alert situations as defined by the agency user, but if a buffer zone is entered, the constant tracking mode is activated to track the participant more accurately and to "catch" them entering the exclusion zone with greater reliability. **IMPORTANT SENTINEL ADVANTAGE:** For one-piece GPS participants, since the OM series it is always active and communicates through cellular coverage real-time participant information, including on-demand location verifications, can be accessed through the software's Location History window **"Current Location" button**. While this on-demand location information is accessed at the time of request, virtually instantaneously, Last Known Location gives the user the fastest information, taking the last point stored and displaying it on the map. The time of the point is given, along with the relative address and latitude and longitude. If more current information is needed, selecting Current Location will instruct the system to contact the device, perform an immediate location and display it on the map. **IMPORTANT SENTINEL ADVANTAGE:** The TrakMate II GPS Tracking Device's ability to provide tracking data at a collection rate of one (1) location point every minute while downloading all information to the monitoring center every five (5) minutes for active, hybrid or passive monitoring. The levels of service are built-in to the software and do not require "change out" or replacement of equipment in order to change an offender's level of GPS supervision. This five (5) minute intensive level of reporting exceeds most active and hybrid reporting levels and far exceeds the requirement for this RFP. Due to this intensive reporting capability, near real-time information is readily available for all active and intermediate GPS tracking participants on an on-going basis virtually eliminating the need for on-demand location capabilities as the average "ping" or "on-demand" location request takes anywhere from two to three (2 – 3) minutes to complete and additional time to report through the cellular networks to the monitoring system.

			Additionally, the SenTrak system is also capable of establishing configurable inclusion and exclusion zones; collecting offender points at a minimum of once every 1-minute; communicating (with the offender); providing location mapping; providing alert notifications and crime correlation (event detection) as described in more detail in the following specification responses.
5.19	System, Software and Mapping	a. establishing configurable inclusion and exclusion zones;	**Sentinel exceeds this requirement.** Through Sentinel's web-based software platform, SenTrak, authorized personnel are able to create, edit and delete exclusion and inclusion zones. SenTrak allows multiple exclusion and inclusion zones per client and numerous schedules per client, including permanent and temporary schedules that can be associated with zones. Zones are created in the SenTrak software as undifferentiated zones and can then be used as inclusion, exclusion or undifferentiated zones depending on a participant's assigned schedule. Sentinel designed SenTrak to allow easy access to zone-setting parameters. Once an offender is selected for a zone assignment, authorized personnel will simply enter the address of the desired zone location and the range perimeter of the zone. Authorized personnel will select if it is to be an exclusion or inclusion zone and then name the zone for later ease of identification. SenTrak visually differentiates zones with color-coding, as follows: Inclusion Zone = **Green**; Exclusion Zone = **Red.** Once the zone has been established, it can be modified any time. As a service feature to customers, this data entry for geographic zones can also be completed remotely by through Sentinel monitoring center personnel. Through SenTrak, authorized users can create multiple zones to cover larger areas, create travel corridors or place zones within zones when required. The SenTrak system allows for zones to overlap and change on a time basis. For example, a person may have to stay in the City of Bismark (Inclusion Zone) but not be allowed near a prior victim's house or any school or park (Exclusion Zone). Exceptions to any zones rules can be created using calendars and time. Sentinel work with each agency on a case-by-case basis to create customized zone templates when needed. Zone templates can also be created where a pre-determined amount of zones are automatically applied to specific offenders or population groups. SenTrak records and reports an offender's entry to and exit from an inclusion as well as an exclusion zone and can immediately report this information. **IMPORTANT SENTINEL ADVANTAGE:** The system provides the ability to

			create buffer zones around exclusion zones of one-piece GPS tracking participants. Buffer zones can be attached to an exclusion zone and can be set at a 50-foot minimum radius with no maximum limit. Once a device is in a buffer zone, the device will automatically activate a constant tracking mode (get location information once every minute and report into the system once every minute) regardless of the participant's monitoring type until the device is located outside of the buffer zone. This capability allows agencies to more accurately track participants entering the exclusion zone with greater reliability.
5.20	System, Software and Mapping	b. collecting offender points at a minimum of once every 1-minute	**Sentinel meets this requirement.** Sentinel offers intensive tracking of offenders at **one point per minute at all levels of tracking (active, hybrid, passive)** and records and stores each point with the date, time and location of the event in the SenTrak software for use in monitoring a participant's compliance with court orders and terms/conditions of probation.
5.21	System, Software and Mapping	c. communicating (with the offender)	**Sentinel meets this requirement.** Sentinel's proposed systems and SenTrak software enable officers to communicate on demand with participants, including the audible/visible/vibration participant alert communications and acknowledgement button of the OM400, as well as text and two-way voice communications with TrakMate II. The most fluid and preferred method of communication is via two-way voice with participants using TrakMate II. **In addition to automated notifications, Sentinel is highly experienced at providing triage services via monitoring center staff whereby live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts.** Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated.
5.22	System, Software and Mapping	d. providing location mapping;	**Sentinel exceeds this requirement.** For GPS participants, real-time and all historical participant information can be accessed through the SenTrak software. Please note: Users have the ability to view historical GPS points for specified date ranges. The mapping history will display every point recorded or it can group points for more clarity.

			 **IMPORTANT SENTINEL ADVANTAGE:** For one-piece GPS participants, since the OM series is always active and communicates through cellular coverage real-time participant information, including on-demand location verifications, can be accessed through the software's Location History window "Current Location" button. While this on-demand location information is accessed at the time of request, virtually instantaneously, Last Known Location gives the user the fastest information, taking the last point stored and displaying it on the map. The time of the point is given, along with the relative address and latitude and longitude. If more current information is needed, selecting Current Location will instruct the system to contact the device, perform an immediate location and display it on the map.
5.23	System, Software and Mapping	e. providing alert notification; and	**Sentinel meets this requirement.** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic officer notification for monitoring participants. Sentinel supports all methods of notification, such as page (alpha or numeric), electronic mail, manual voice phone call, and/or text message to a cell phone. Privacy rules can be configured to ensure all participant and user data is kept confidential. SenTrak also allows for authorized personnel to determine alarm and notification protocols. Prior to deployment, Sentinel's operations team can meet with department personnel to establish group level alarm and notification protocols. Once these groups, such as "high risk", are established, the department can place individuals within the specific group and receive alarms and notifications as dictated by the pre-determined protocols for that group. The

			agency can set instantaneous response, end of day notification summary or no notification requirements. Sentinel will work with each Western States Contracting Alliance participating agency to ensure all notifications are customized to meet personnel schedules, set work day hours, off time, etc. to guarantee the appropriate response times to ensure public safety.
5.24	System, Software and Mapping	The Vendor's system shall have the capability to query GPS location information both automatically and individually, including latitude and longitude, and mapping on all defendants/offenders based on specified distance from a specified location within specified date/time range as means of performing analysis of GPS Offenders at a potential crime scene.	**Sentinel meets this requirement.** Sentinel's SenTrak web-based monitoring application features a built-in "event detection" platform for all multi-piece GPS tracking participants. By incorporating this application into Sentinel's main portal offers the agency the capability to initiate a query against one participant or the entire population of participants on GPS tracking in just a matter of minutes. **Authorized personnel can enter the date, time and location of any incident and promptly receive a report of all participants who were near the location.** The results of the query can also be graphically displayed on an individual map allowing the event and plotted participant information, relative to the query, to be viewed. Authorized personnel are able to perform these searches at any time from any internet–enabled computer. A "results" table is generated depicting all participants who were within the proximity of the incident. **This map distinguishes the incident location by placing a red star upon the location. Each participant within the specified radius of the incident is identified. This report can be viewed on screen or printed for later review.**

			IMPORTANT SENTINEL ADVANTAGE: All "event detection" participant, geographic, and latitude and longitude data can be exported and provided to multiple law enforcement agencies for cross reference with their own internal and/or proprietary mapping software. This software option is provided at **no cost** to the agency. This Sentinel solution can also provide crime correlation data to check the proximity of any one-piece GPS participant to any specified location(s) at any historical time. The SenTrak software has, through the use of Proximity Report utility to show if a target offender or offenders were in proximity of a particular address or location of a crime. This report can be generated by simply entering an address of interest including a crime incident report address and running the report. These reports will stay within the system until a new address is entered but saved indefinitely for a permanent record through exporting the report to Excel. The Proximity Report shows the name of the offender, the date and time, Latitude, Longitude, Distance to the address, the specific address identified, the offender device ID as well as an active link to view the tracking points via mapping for each participant identified by the query.
5.25	System, Software and Mapping	The Vendor's system software shall allow for a non-erasable alpha numeric identification designated by the Agency. A unique identification shall be used for each offender within the Vendor's system. In addition, the software shall require the following minimum mandatory fields for initial offender enrollment:	**Sentinel exceeds this requirement.** Using SenTrak officers can profile new participant enrollments. To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's name, agency designated unique alpha-numeric identifier, physical address, serial number of assigned equipment, time zone, assigned officer, and offender photo. In addition to entering the basic requirements, an agency can choose participant demographic information, offers free field fields and allows agencies to request customized fields for additional agency specific participant information. Sentinel is the original developer of SenTrak and Sentinel engineers control the web-based data fields, reports and queries, ensuring Sentinel is fully capable of meeting agency data and reporting needs. As an additional benefit, users can enroll participants in the system and activate them at a later date. Agency officers, equipment installers or authorized monitoring personnel can activate the saved enrollment upon notification of in-home equipment installation or on the participant's scheduled start date. Users also have the ability to terminate a participant's monitoring through the SenTrak. The SenTrak system provides authorized staff with the ability to force resolution when terminating clients from the system. Additionally, SenTrak users can schedule one-piece GPS tracking participant's terminations for a time

			in the future.
5.26	System, Software and Mapping	a. name;	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's name.
5.27	System, Software and Mapping	b. unique numeric identifier;	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's agency-designated unique alpha-numeric identifier.
5.28	System, Software and Mapping	c. physical address;	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's physical address.
5.29	System, Software and Mapping	d. serial number of equipment;	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the serial number of assigned equipment.
5.30	System, Software and Mapping	e. time zone;	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the monitoring time zone.
5.31	System, Software and Mapping	f. assigned officer; and	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements which include the participant's assigned officer.
5.32	System, Software and Mapping	g. offender photo.	**Sentinel meets this requirement.** To complete a participant's enrollment for monitoring, Sentinel has established basic entry requirements that may include the participant's photo.
5.33	System, Software and Mapping	The Vendor's mapping software utilized shall include but not be limited to the following:	**Sentinel meets this requirement.** SenTrak mapping software has the capability to allow unlimited automatic access to the most up to-date maps available with state-of-the-art graphics with aerial photography capabilities; allow for zooming/scaling from street level to statewide; allow for identification/labeling of streets; display offender location information in a sequenced event and/or at a specific date and time; and display inclusion and exclusionary zones that shall be printable from the screen. Please see the following specification responses for more specific information.
5.34	System, Software and Mapping	a. Allow unlimited automatic access to the most up to-date maps available with state-of-the-art graphics with aerial photography capabilities.	**Sentinel exceeds this requirement.** Bing Maps and Google Maps® provide automatic updates to the SenTrak mapping software providing the latest in maps and upgrades at all times. Sentinel does not maintain maps within the SenTrak mapping software, unlike some vendors who must download regular updates to their mapping software– a very time consuming process. SenTrak tracks all location points and overlays the one-piece GPS tracking points on the most recent Bing Map available and the multi-piece GPS tracking points on the most recent Google Map available at the time of the tracking.

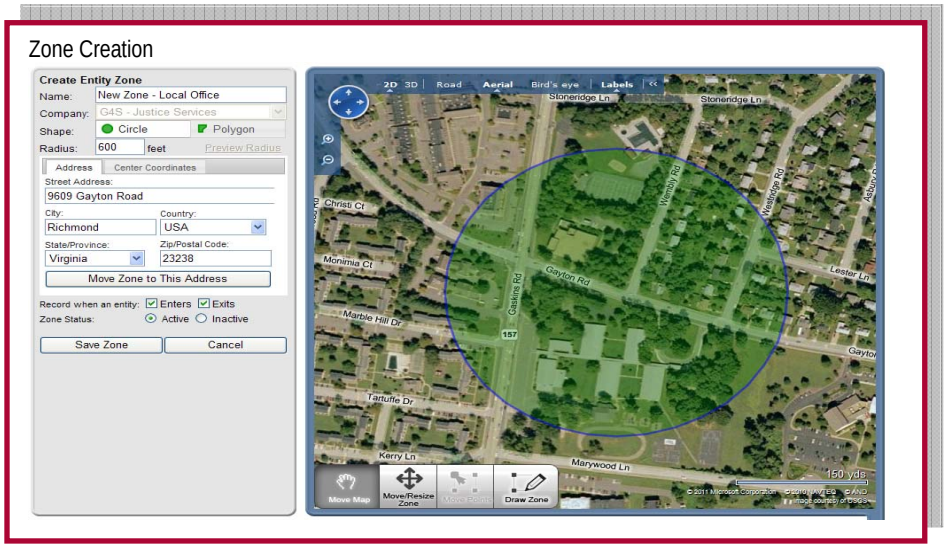
			Both Google Maps and Bing Maps have state-of-the-art graphics including aerial mapping capabilities and much more. For example, Bing Maps utilized with the one-piece GPS tracking solution can be view in aerial, road, 2D, 3D and Bird's Eye views and can show state, county, municipality and street names at the discretion of the user. The interactive maps featured in the software have the capability to display the physical location of participants with varying degrees of detail through the zoom feature. The SenTrak software will allow agency personnel to easily zoom in and out on any map by dragging the mouse to designate an area and clicking "+" or "-" or by using the mouse roller. All maps are easily moved by clicking on the area of interest and dragging the mouse to the center of the screen. The Additionally, the SenTrak software will allow the agency personnel to play, pause, stop, fast-forward and rewind the location history of any one-piece device.
5.35	System, Software and Mapping	b. allow for zooming/scaling from street level to statewide;	**Sentinel meets this requirement.** The SenTrak software will allow agency personnel to easily zoom in and out on any map from street level to statewide by clicking "+" or "-" or by using the mouse roller. All maps are easily moved by clicking the area of interest and dragging the mouse to the center of the screen.
5.36	System, Software and Mapping	c. allow for identification/labeling of streets;	**Sentinel meets this requirement.** The mapping application (maps) utilized in the SenTrak software contain easily recognizable images at the global level, state level, and down to street level; in addition, authorized users can select to view labels of places of interest, landmarks, schools or street names to the mapping system.

5.37	System, Software and Mapping	d. display offender location information in a sequenced event and/or at a specific date and time; and	**Sentinel exceeds this requirement.** Users have the ability to view all historical GPS points for participants during specified time periods or at any specific date and time. The mapping history will display every point recorded or it can group points for more clarity. All sequenced location points will be numbered or designated with a directional arrow to show the movement of the participant. **IMPORTANT SENTINEL ADVANTAGE:** The SenTrak software also allows a user to view location history in an easy-to-read spreadsheet format giving each one-piece GPS device's location point time, address, longitude, latitude and accuracy. Additionally, one-piece GPS device's Location histories can be exported to Excel to show every point or groups as well, at the user's discretion, allowing for the data to be easily transferred to the agency's crime analysis software. **IMPORTANT SENTINEL ADVANTAGE: The software allows agencies to run a Movement Report on one specific one-piece GPS participant or on groups of one-piece GPS participants.** This report will show the participant's name, the start and stop time of the movement, the duration of the movement, the distance of the movements, the duration of any stops and the maximum speed

			attained during the movement. This report can be integral in assisting the WSCA participating agencies with determining if certain groups of offenders (known gang members or criminal cohorts) are abiding by the terms of their monitoring and refraining from contact.
5.38	System, Software and Mapping	e. display inclusion and exclusionary zones that shall be printable from the screen.	**Sentinel meets this requirement.** The mapping component of the software will allow agency personnel to **print any mapping screen** including a display of inclusion and exclusionary zones through the standard print function on the Internet browser. As an additional benefit GPS tracking reporting and testimony purposes, the software will allow users to print both the map with visual confirmation of a participant's location history along with a list of each location point of the same sheet of paper.
5.39	System, Software and Mapping	The Vendor's system shall 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.	**Sentinel exceeds this requirement.** Through Sentinel's web-based software platform, SenTrak, authorized personnel are able to create, edit and delete exclusion and inclusion zones. SenTrak allows multiple exclusion and inclusion zones per client and numerous schedules per client, including permanent and temporary schedules that can be associated with zones. Zones are created in the SenTrak software as undifferentiated zones and can then be used as inclusion, exclusion or undifferentiated zones depending on a participant's assigned schedule. Sentinel designed SenTrak to allow easy access to zone-setting parameters. Once an offender is selected for a zone assignment, authorized personnel will simply enter the address of the desired zone location and the range perimeter of the zone. Authorized personnel will select if it is to be an exclusion or inclusion zone and then name the zone for later ease of identification. SenTrak visually differentiates zones with color-coding, as follows: Inclusion Zone = **Green**; Exclusion Zone = **Red.** Once the zone has been established, it can be modified any time. As a service feature to customers, this data entry for geographic zones can also be completed remotely by through Sentinel monitoring center personnel. Through SenTrak, authorized users can create multiple zones to cover larger areas, create travel corridors or place zones within zones when required. The SenTrak system allows for zones to overlap and change on a time basis. For example, a person may have to stay in the City of Bismark (Inclusion Zone) but not be allowed near a prior victim's house or any school or park (Exclusion Zone). Exceptions to any zones rules can be created using calendars and time. Sentinel work with each agency on a case-by-case basis to create customized zone templates when needed. Zone templates can also be created where a pre-

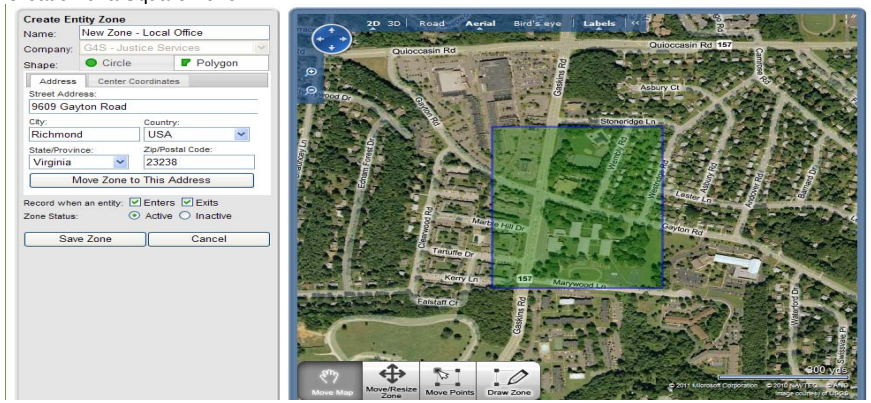
determined amount of zones are automatically applied to specific offenders or population groups. SenTrak records and reports an offender's entry to and exit from an inclusion as well as an exclusion zone and can immediately report this information.

To create a zone for a specific one-piece GPS participant, officers simply select Zones from the Manage Offender option in SenTrak, name the zone, select the shape of the zone (circle or polygon), select the zone radius in feet and enter either the address or coordinate position of the zone (latitude/longitude).



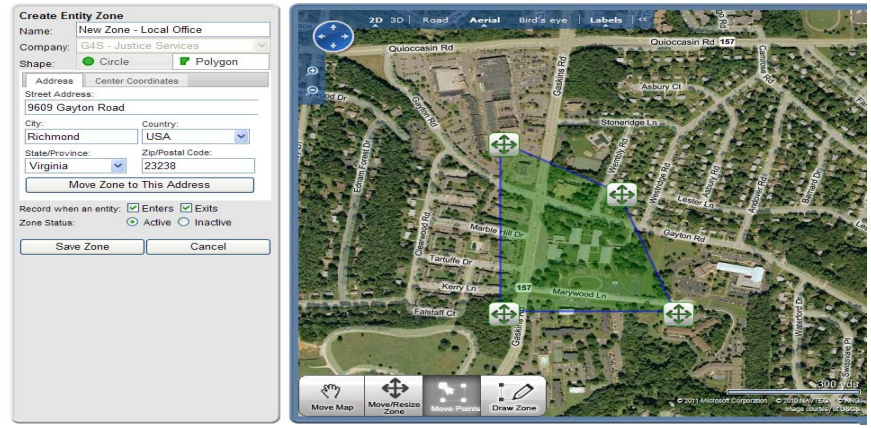
Please note the previous example showed the creation of circular zone, however agencies will also be able to create square or polygon shaped zones. To create a square zone, officers have to simply toggle from a circular shape to a polygon shape.

Creation of a Square Zone



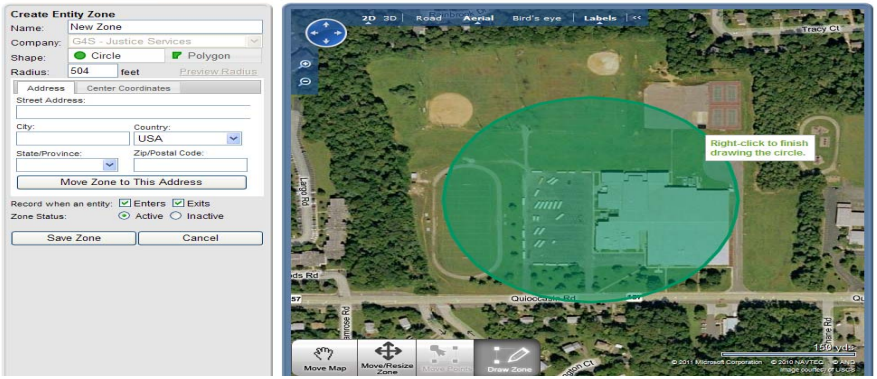
After making the zone a square, officers can select the Move Points button on the mapping screen and reshape the zone as desired.

Creation of a Polygon Zone



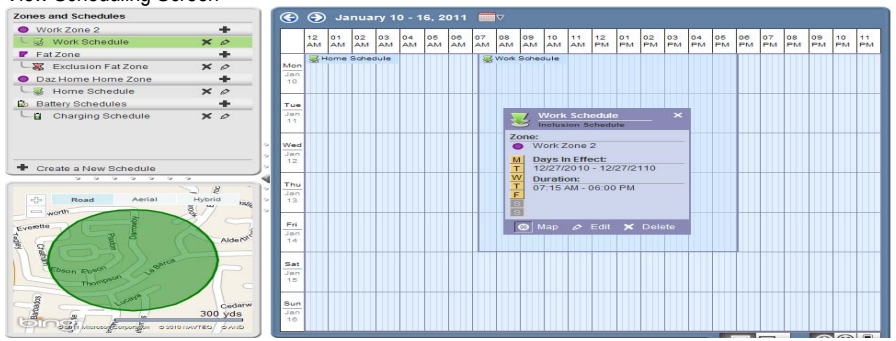
IMPORTANT SENTINEL ADVANTAGE: The proposed solution allows agencies several options for zone creation including the ability to draw zones on the map around geographical landmarks. The map below is an example of an aerial view with geographical locations, state, county, municipality and street names which can be displayed at the discretion of the user when using the drawing tool for zone creation.

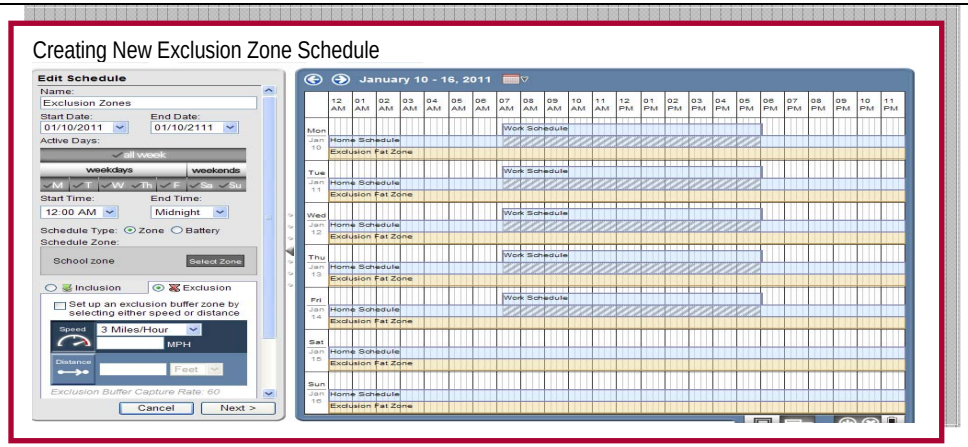
Zone Creation on the Map around Geographical Landmarks through the Drawing Tools



The SenTrak system will allow authorized users to create, edit and delete all parameters for individual participants. Additionally, the system will allow approved staff the ability to apply monitoring schedules and zones for entire groups of participants. .

View Scheduling Screen



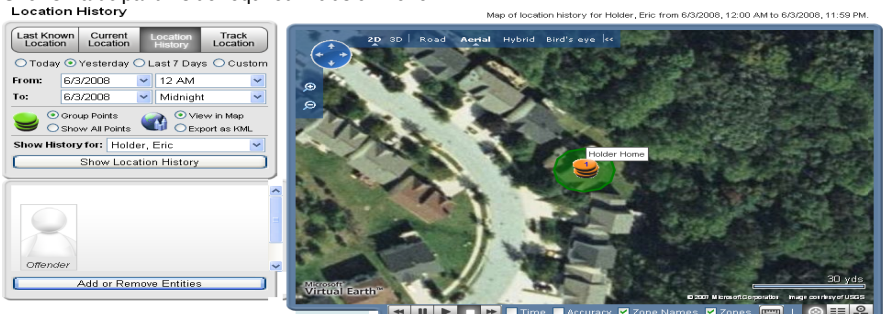


Time exceptions to these schedules can also be created using an easy to use calendar. Additionally, monitoring changes subsequent to installation can be completed through the SenTrak software and do not require interaction with the participant. Officers are alerted when participants are not where they should be during a specified time or if they get too close to an exclusion zone.

Additionally, the system allows users to easily **modify** curfew schedules and GPS zones on a per-participant basis remotely at any time by clicking the Edit Icon (pencil) on the Completed GPS Schedule Screen.

IMPORTANT SENTINEL ADVANTAGE: The software will allow the agency to create unlimited schedules for participants and apply inclusion or exclusion zones to these schedules. The following are examples of inclusion and exclusion zones:

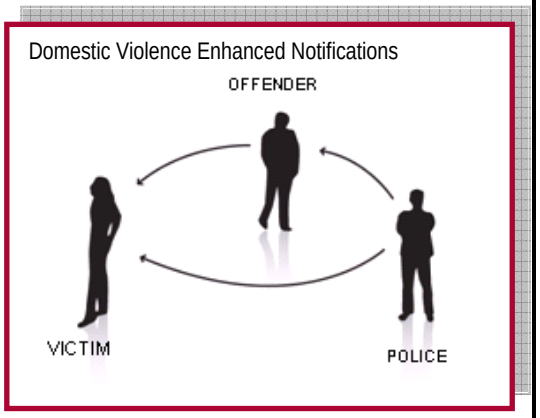
Shows Participant inside required Inclusion Zone



Exclusion Zone with Zone Breach

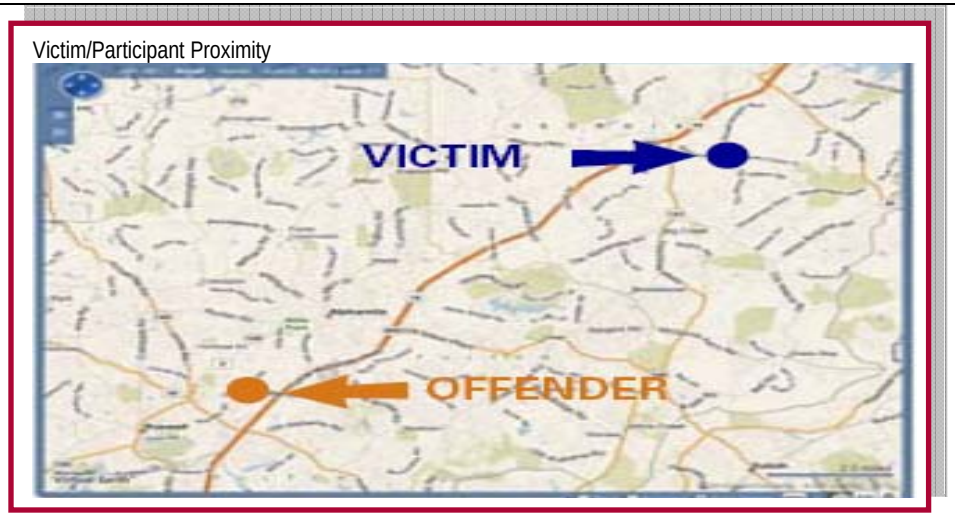
IMPORTANT SENTINEL ADVANTAGE: The combination of a one-piece tracking device worn by the offender plus a secondary device carried by the victim creates a unique "Mobile Exclusion Zone" around the victim (as referred to by the WSCA RFP as "Proximity Zone"). This system is integrated into the tracking software and can notify the victim as well as law enforcement if the abuser gets too close to the victim 24 hours, seven (7) days a week regardless of location. This technologically advanced system of tracking domestic violence offenders' proximity to victims, regardless of location. This Mobile Victim Zone capability has proven has been highly successful in multiple locations throughout the nation, including but not limited to: Illinois, Michigan and Connecticut, and has helped them to become leaders in the fight to end domestic violence.

For participant/victim tracking applications, most vendors only offer inclusion and exclusion zones around fixed locations and offer no coverage for the victim at common times when they are mobile. Sentinel has led the charge for domestic violence monitoring with the solution Sentinel is presenting which was specifically designed for domestic violence situations and has the capability to establish Mobile Exclusion Zones around people rather than simply locations. The Sentinel participant/victim tracking solution is highly unique. Agencies will have the ability to create "Mobile Victim Zones" (as referred to by the WSCA RFP as "Proximity Zone") zones that are established around a **secondary monitoring device that is voluntarily carried by the victim at all times**. One (1) truly unique capability of the Sentinel solution is that Sentinel can alert victims, judges, witnesses or other people of interest **in real time** about the proximity to a participant by tracking the victim's tracking device relative to the participant's tracking unit. If a domestic violence or restraining order victim chooses to carry a tracking device, the software will then track the victim's tracking device to provide real time alerts to the victim and law enforcement when the offender comes within the agency-defined proximity.



The system can alert the officers, offenders and/or victims through automated voice alert and/or text message to a mobile phone and/or home phone regarding the location of the offender and/or alert the victim. As an alternate service, these system alerts can be rapidly routed to a specialized team of live Sentinel monitoring center staff who are dedicated to promptly initiate calls to offenders, victims and/or officers to triage alerts and provided directions or guidance in observing

			the proper distances of separation specified by court and notify officers and/or law enforcement regarding confirmed non-compliance. Alerts are most commonly created in the following scenarios: ▪ **Mobile Exclusion Zone Violation:** This occurs when an offender's ankle device enters a user defined zone around the victim's tracking device. For instance, if the offender is ordered to stay a certain distance away from someone, such as a victim, witness, or former cohort, then a violation would occur if the offender's ankle bracelet came within that distance of the secondary tracking device carried at all times by the victim, witness, or cohort. ▪ **Mobile Buffer Zone Violation:** The officer has the ability to establish a buffer zone around a mobile exclusion zone therefore allowing for early detection of potential violations. For example, if a victim has a 1,000 foot mobile exclusion zone around his/her device, the officer can choose to establish an additional buffer zone of any size and receive notification if the offender enters this buffer zone. This allows for early detection and notification of potential violations ensuring victim safety and offender compliance. The Sentinel participant/victim tracking solution gives officers the ability to continuously monitor a participant's proximity to their victims. The locations of the participant and the victim are recorded as historical data giving officers insight into how much time a participant is spending in the vicinity of a victim.

			
6.0	**SECTION F System Reports**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
6.1	System Reports	System Reports shall allow the Agency to generate the following "canned" reports directly from the Vendor's database through the secure internet site.	**Sentinel exceeds this specification.** Authorized users have the ability to directly access all participant historical information through Sentinel's secure web-based monitoring platform, SenTrak. All monitoring standard reports are available through the proposed software's easy-to-use report generator applications in standard transaction file formats. **IMPORTANT SENTINAL ADVANTAGE:** Additionally, Sentinel catapulted the speed, capacity and capabilities of monitoring software through the development of the SenTrak SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective.
6.2	System Reports	To ensure that reports are accurate and timely, the system's database shall be updated in real time to ensure all report data is current when viewed and/or downloaded by the Agency's personnel.	**Sentinel meets this requirement.** Any authorized user can view and /or download participant activity data 24 hours a day, seven (7) days a week, 365 days a year. Participant activity is posted **in real-time**, so that agencies always have the latest information and users can view tracking information and violations online as they occur. Additionally, Sentinel will provide all written reports to the agencies as needed to operate an efficient and effective program including but not limited to daily participant activity reports for each program participant, alert/violation reports, and monthly summary inventory reports.

6.3	System Reports	All reports shall have the capability of being queried, sorted or filtered by any field contained in the report or by data parameters as applicable and reports shall be readable on screen, printable and shall be downloadable into an excel format.	**Sentinel meets this requirement.** Sentinel designed its proprietary, web accessible monitoring software, SenTrak, specifically for use in the offender services arena. Employing SenTrak allows **real-time, on-line web accessibility to participant tracking information and reports** for Sentinel employees **and** authorized participant agency and/or court personnel. **The software allows for unlimited reporting capability where the users customize and filter several categories specific to the reports.** Some examples of customization including the reporting data range (start and end dates), types of log (event, alert or information, maximum speed limit, length of stops, and the entities to be reporting by individual participant, several selected participants, or groups of participants (i.e. active/inactive or offender/victim/witness). **Additionally, all alert data from the database can be exported to Microsoft Excel at any time for further customization and sorting based on user-defined parameters** Additionally for its multi-piece GPS tracking participants, Sentinel catapulted the speed, capacity and capabilities of monitoring software through the development of the SenTrak SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective.
6.4	Equipment Inventory Reports	The system must be able to provide real time reports of all assigned equipment. Report shall include description/type of equipment, serial number, assigned Offender, and assigned Officer.	**Sentinel meets this specification.** Sentinel will provide the agency with monthly, weekly or on-demand reports of all inventory in the agency's possession. For the purposes of inventory reconciliation, the report will include description/type of equipment, serial number, assigned Offender, and assigned Officer as well as an inactive inventory assigned to the agency. Additionally, SenTrak will generate **a D**evice Report on-demand for one-piece GPS tracking units showing a view of all inactive and active units.
6.5	Notification Report	The Vendor's system shall provide the Agency the ability to generate a report by date parameters, sorted by location site, identifying the number and type of notifications during specified time parameters, such as: • Monday-Friday, 8:00 am-5:00 pm • After hours • Weekends And indicating summary totals for: • total number of alerts per location	**Sentinel meets this requirement.** Summary alert information by location site, individual assigned offender **or group of offenders** is available through SenTrak for specified time periods and available for viewing, printing or saving 24 hours a day, seven (7) days a week, 365 days a year. These can identify the type of alert, time of alert, method of alert (fax, e-mail or phone call) and recipient of alert or be customize as required based on each participating agency preference. Currently, SenTrak will generate the following standardized one-piece GPS tracking reports immediately and on an on-going basis directly through the software with no monitoring center intervention.

		site, • percent of total per type of alert and average number of alert notifications per month, • per offender within each location site.	▪ Alert Report: Gives a history of all alerts associated with one (1) or more participants ▪ Event Log: Gives a history of all alerts, events and a log of information ▪ Alert Summary Report: Provides a statistical view of alert types by volume Additionally, SenTrak's "Group Reports/Alert" function allows authorized personnel to display their active multi-piece caseload by alert status. The "Group Status by Alert Report" function shows all offenders whose alerts are unresolved. The "Group Violation Reports by Category" function provides all violation activity ordered by category for a selected time period. Sentinel can also continuously make available the following multi-piece reports: ▪ Individual ✓ All activity ✓ Violations only ▪ Group ✓ All activity ✓ Violations by Individual ✓ Violations by Category
6.6	Offender Alert Report	The Vendor's system shall provide the Agency the ability to generate alert reports, queried by individual assigned offender and date parameters that identifies the type of alert, time of alert, method of alert (fax, e-mail or phone call) and recipient of alert.	**Sentinel meets this requirement.** Summary alert information by individual assigned offender **or group of offenders** is available through SenTrak for specified time periods and available for viewing, printing or saving 24 hours a day, seven (7) days a week, 365 days a year. These can identify the type of alert, time of alert, method of alert (fax, e-mail or phone call) and recipient of alert or be customize as required based on each participating agency preference.
6.7	Customized Reports	The Agency can request custom reports the cost of which (if any) shall be established between the Vendor and the Agency Program Manager.	**Sentinel meets this requirement.** Sentinel designed its proprietary, web accessible monitoring software, SenTrak, specifically for use in the offender services arena. Employing SenTrak allows **real-time, on-line web accessibility to participant tracking information and reports** for Sentinel employees **and** authorized participant agency and/or court personnel. As the SenTrak monitoring software is an in-house concept and design, SenTrak is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support and recommends all participating stakeholders have access to the SenTrak software for program review and oversight.** Sentinel catapulted the speed, capacity and capabilities of monitoring software through the development of the SenTrak SQL database system. The SQL

			database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective. **This translates into the ability to modify or develop new software variations as may be needed for the agency directly, in house, without having to utilize outside vendors which may bring data security concerns to the agency. Only Sentinel personnel would have access to the confidential participant data and the development of any new application.**
6.8	Offender Report	The Vendor's system shall provide the Agency the ability to generate a summary report of all offenders and/or assigned officer that identifies offender name, Agency number, address, and officer assigned.	**Sentinel meets this requirement.** Sentinel can provide any authorized participating agency personnel a summary report of all offenders and/or assigned officer that identifies offender name, agency identifier, address, and officer assigned. Based on requests from correction administrators for top-level program statistics, Sentinel developed custom software to extract broad level program data for custom reports. These optional reports provide program administrators the ability to analyze all offenders and/or assigned officer per agency, per office and per caseload basis in an "on-demand" basis or at regular specified intervals (commonly monthly, quarterly, semi-annually and annually). These optional reports have proven beneficial to program administrators as a means to better manage resources, identify trends in supervision and as a tool to balance caseloads among line staff. Sentinel will work with its clients to ensure all needed reports, including on-demand reports, daily and quarterly reports are available.
6.9	Current Usage Report	The Vendor's system shall be able to provide the Agency the ability to generate a current usage report indicating the actual number of daily service units used to date (real time) for the monthly period. This report should be detailed to reflect offender name, Agency number, service type (active) and number of days utilized to date.	**Sentinel meets this requirement.** Sentinel can provide any authorized participating agency personnel current usage reports indicating the actual number of daily service units used to date (real time) for any monthly period. This report can include but is not limited to offender name, agency number, service type (active) and number of days utilized to date (real time) for the monthly period on demand or through the SenTrak software. For example, currently through SenTrak, agencies can view, print or save an "Enrollment Summary" report for all multi-piece GPS tracking participants that is a two-page report designed to provide a daily recap of program participants who enrolled during a specific period. The first page contains information about all new clients added that day, and all clients deleted due to program completion or program revocation. Sentinel will distinguish in this report between completions and revocations to ensure a statistical basis for measuring the overall effectiveness of the electronic monitoring program may be maintained. This will

			assist in the preparation of statistics that may be used by agency personnel for other reports or studies. The second page of this report contains the name, unit number, and enrollment date of every client being monitored on that day. This report will allow the agency to review the actual participant count on a daily basis and will track "year-to-date" total participant count information for statistical purposes.
6.10	Daily Alert Summary Report	The Vendor shall submit a daily report (between the hours of midnight and 6:00 a.m. for the previous day) that identifies each alert, type of alert, time and duration of alert, assigned officer, assigned offender, and totals. This report shall be sorted by location sites region/unit/officer and shall be e-mailed to all designated officers within the location sites.	**Sentinel meets this requirement.** Sentinel monitoring system will automatically send a daily report via email or fax between the hours of midnight and 6:00 a.m. for the previous day's GPS tracking alert. The report will minimally identify each alert, type of alert, time and duration of alert, assigned officer, assigned offender, and totals to each participating agency as is applicable based on agency utilization and notification/reporting requirements. This report can be sorted by location sites region/unit/officer and sent to all designated officers within the location sites. **IMPORTANT SENTINEL ADVANTAGE:** Summary alert information is also available through SenTrak for specified time periods and available for viewing, printing or saving 24 hours a day, seven (7) days a week, 365 days a year.
7.0	**SECTION G Equipment Testing, Replacements, Lost/Damaged/Stolen Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
7.1	Ongoing Demonstration/ Testing Equipment	The Vendor shall allow the Agency the use of five (5) GPS monitoring units or systems for demonstration and/or testing purposes, not to exceed a ten (10) day period for any single demonstration/test period. These units/systems shall not be part of the backup inventory and shall be provided at no additional cost. Units/systems may be demonstrated/tested at the discretion of the Agency.	**Sentinel meets this requirement.** Sentinel will provide each participating agency the use of five (5) GPS monitoring units or systems for demonstration and/or testing purposes, not to exceed a ten (10) day period for any single demonstration/test period at the discretion of the agency. Sentinel understands these units/systems are not a part of the backup inventory and shall be provided at no additional cost.
7.2	Equipment Accessories	The Vendor shall provide (when necessary or upon request depending on the item) all necessary GPS tracking supplies and replacement supplies, including but not limited to; straps, clips, batteries, installation-removal	**Sentinel meets this requirement.** Sentinel will provide all necessary GPS tracking supplies and replacement supplies, including but not limited to; straps, clips, batteries, installation-removal equipment supplies, beacons or other RF monitoring units, car chargers, charger base or cords and instruction/training materials when necessary or upon request.

		equipment supplies, beacons or other RF monitoring units, car chargers, charger base or cords and instruction/training materials.	
7.3	Equipment Spare Inventory	The Vendor shall provide and maintain a backup/replacement inventory of monitoring units or systems up to fifteen percent (15%) of the actual number of units/systems currently in use in each the Agency's Location sites/Office locations at no additional cost. The Agency shall not pay the Vendor an inventory fee, storage fee, installation equipment fee or any other fee related to these inventory units and equipment.	**Sentinel meets this requirement.** Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. Sentinel understands that no agency will be required to pay an inventory fee, storage fee, installation equipment fee or another fee related to inventory units/spare equipment. Sentinel acknowledges that participating agency only for the per-day unit rate on activated units as set forth in the contract.
7.4	Replacement Equipment	The Vendor shall assure that all equipment delivered to the Agency has been tested to ensure it is operable, free from any defects or damage and is fully operational. The Agency reserves the right to reject any and all equipment not determined to be operational and in acceptable operative order and condition. In the event any equipment becomes inoperative due to a malfunction or through normal use, the Vendor shall incur all replacement costs and repairs. The Vendor shall provide the Agency with replacement equipment within 24 hours at no charge to the Agency, including shipping and handling costs for both delivery and return.	**Sentinel meets this requirement.** Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems and confirms that all equipment provided to WSCA participating agencies will be covered by a full manufacturer's warranty **for the length of any contract**. Sentinel will maintain all equipment in good operating condition, free from materials defects and/or workmanship under normal use and fully operational for the term of this agreement. Sentinel understands that the participating agencies reserve the right to reject any and all equipment not determined to be operational and in acceptable operative order and condition. Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. Sentinel's assigned Account Manager will work proactively with each Western States Contracting Alliance participating agency to ensure the appropriate amount of equipment and spares are maintained for the electronic monitoring of offenders. This open communication allows Sentinel to provide equipment in a timely manner without having to depend on costly overnight / express delivery in order to meet the program's equipment needs. In the event of any malfunction of any piece of equipment, Sentinel will provide routine equipment maintenance repair through the return and replacement of

			malfunctioning equipment at no additional cost to participating agencies. Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. **Additionally, if any agency's spare inventory is depleted, Sentinel will re-supply the appropriate equipment via overnight delivery at no additional cost within 24 hours after notification.** All shipping costs (both delivery and return) of all equipment and supplies will be the responsibility of Sentinel. **Product Warranty:** Sentinel represents and warrants that, upon delivery of any product and/or consumable to the delivery location, such product will have been manufactured, filled, packaged, stored and shipped materially in accordance with the specifications or custom specifications for such product in accordance with the associated purchase order. Sentinel further represents and warrants that it shall obtain and maintain all necessary licenses, permits or approvals in connection with the manufacture, filling, packing, testing, storage and shipment of each such product. **Sentinel warrants all of its equipment and software for the life of the contract.** This includes software maintenance, licensing and future feature enhancements. **Warranty Service:** Warranty service with Sentinel is a very simple process. The participating agency only needs to contact the proposed Account Manager to discuss warranty service and/or feature upgrades. Sentinel is committed to the continual development of feature enhancement and product development. The Account Manager will also work with the Sentinel training department to provide any training required by a new feature or upgrade to the equipment or system.
7.5	Lost/Damaged/Stolen	At no additional cost, the Vendor shall supply replacements for lost, stolen and damaged equipment up to five percent	**Sentinel meets this requirement.** Sentinel will provide an annual 5% allowance of the daily average of active units per year to each Western States Contracting Alliance participating agency for lost, damaged and/or stolen equipment

		(5%) per year of the Agency's active units/systems. The Vendor shall have three (3) working days to replenish requested stock. All units shall be maintained at the Agency's office for use as immediate replacements, when needed. Vendor must detail within their Price Sheet the per component replacement cost for each component of every proposed equipment model.	replacements. Sentinel requests the opportunity to work closely with each participating agency to ensure programmatic and participant policies achieve this level. Based upon Sentinel's experience in other contracts, Sentinel has found a few points essential to improved management of equipment inventory and loss, damaged or stolen equipment. This includes increased emphasis to not remove the transmitter until all pieces of equipment provided to the participant are together in the same place, either at the participant's home or the participating agency office location. Sentinel would request ongoing coordination with participating agency for participants to return equipment to the participating agency office. Additionally, Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment and will be replenished within three (3) working days should the stock become depleted. Sentinel has provided the per-component cost for lost, stolen or damaged replacement equipment in excess of the annualized 5% allowance in the pricing section of this proposal should payment be required.
8.0	**SECTION H Training Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
8.1	On-Site Initial Training	Vendor shall provide initial on-site training by experienced staff with thirty (30) days of start of Agency's contract, unless an alternate training schedule is agreed upon. Additional on-site training via webinar shall be provided within 48 hours of request. Ongoing training shall be provided as agreed mutually between vendor and agency.	**Sentinel meets this requirement.** Sentinel is committed to working in partnership with each participating agency utilizing the Western States Contracting Alliance contract over the term of the contract to make sure that all staff are fully and properly trained on the operation and installation of the proposed equipment, the use of the software for participant management, and interpretation of violation notifications and reports along with all other needed training requirements. Sentinel will provide initial on-site training has included a sample written training curriculum in the Exhibits section of this proposal for the Western States Contracting Alliance to review and consider. Initial on-site training will be enacted prior to the implementation of the services. In Sentinel's experience, initial training should be conducted in near-proximity to

			intended program start date and be conducted to ensure that all agency personnel are completely comfortable and knowledgeable in using the proposed equipment and systems therefore Sentinel will provide initial training within 30 days of the Notice to Proceed commencement date, unless an alternate training schedule is agreed upon. Initial training includes instruction on the operation of any monitoring equipment and software discussed in this proposal and selected for use and implementation by the respective participating agency. Once Sentinel management and participating agency management agree upon program guidelines, notifications, and parameters, Sentinel will arrange for a mutually beneficial training session. Additionally, Sentinel will provide post-deployment on-going training per the established contract at no cost to the participating agency. Any future training will be scheduled in a manner that is beneficial and cost-effective to both the agency and Sentinel. **IMPORTANT SENTINEL ADVANTAGE:** The Sentinel training department offers webinar training sessions for customers and staff on an on-going basis. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
8.2	On-Site Initial Training	Deleted.	
8.3	Onsite Ongoing Training	Deleted.	
8.4	Manuals/ Installation Guides	The Vendor shall provide training and/or user manuals upon each Officer's initial orientation training in hardcopy or soft file format such as PDF may be provided at the request of the Agency. All training and all associated training manuals shall be provided at no cost to the Agency.	**Sentinel meets this requirement.** Sentinel will supply all operational/procedural manuals and training materials, including written instructions and equipment for initial training, to be used by participating agency personnel at no additional cost. Sentinel will also provide all training and/or user manuals in hardcopy or soft format (such as PDF) and provide written authorization to the participating agency to duplicate these materials as necessary to facilitate future agency training needs.
8.5	Training Materials	The Vendor shall provide all materials and equipment necessary to perform the	**Sentinel meets this requirement.** Sentinel will supply all operational/procedural manuals and training materials, including written

		training and shall utilize actual equipment currently being utilized. All training manuals may be hardcopies or soft file format, user friendly, and kept up to date with the most current training protocols. Training manuals shall be provided for each Agency staff member trained and upon the request of the Agency Program Manager. The training curriculum and evaluation forms that will be utilized for all training purposed should be submitted by Vendor.	instructions and equipment (actual equipment currently being utilized) for initial training, to be used by participating agency personnel at no additional cost. Sentinel will also provide all training and/or user manuals in hardcopy for each agency staff member trained upon the request of the agency Program Manager or in soft format (such as PDF) and provide written authorization to the participating agency to duplicate these materials as necessary to facilitate future agency training needs. Sentinel confirms all training manuals are user friendly, and kept up to date with the most current training protocols. Sentinel has included a sample written training curriculum and evaluation forms in the Exhibits section of this proposal for the Western States Contracting Alliance to review and consider.
8.6	Webinar and Online Training	The Vendor shall make available to officers remote webinar and online training sessions which demonstrate device applications after initial orientation per officer. The Vendor shall provide Webinar online and online. Training for system, software and hardware updates.	**Sentinel meets this requirement.** The Sentinel training department offers webinar training sessions for customers and staff on an on-going basis address attrition and additional training needs as well as for any system, software and hardware updates. Webinars are offered for all technologies including those proposed herein. These webinars are offered based on internal training calendars, individual training needs, and scheduled on-demand. When an on-demand training need arises, a training request form is sent to the training department. The request is received and assigned to a Training Specialist. The Training Specialist will communicate with the Account Manager and the customer contact to schedule the requested training within 48 hours of request. Once the webinar invitation has been created, it will be sent to the customer contact and the Account Manager. Webinars are conducted based on contract specifications and/or training needs.
9.0	**SECTION I Additional Requirements**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**
9.1	Vendor Staff	The Vendor shall provide an adequate level of staffing for provision of the services outlined herein and shall ensure that staff providing services are highly trained and qualified.	**Sentinel exceeds this requirement.** Sentinel **operates** both its primary monitoring center located in Irvine, California and its geographically diverse secondary back-up monitoring center in Atlanta, Georgia. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Irvine, California that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis. Additionally, Sentinel operates a secondary redundant electronic monitoring center in Atlanta, Georgia that is fully operational and staffed during normal business hours and capable of being promptly staffed 24 hours a day in the event of a failure at the primary monitoring center warranting failover to the secondary/backup monitoring center. **As such, staffed**

			monitoring services and technical support are available through a toll-free telephone number from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. **IMPORTANT SENTINEL ADVANTAGE:** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** Sentinel is proud to state that in its 20 years of operation, it has **never experienced a monitoring center failure or service catastrophe.** **IMPORTANT SENTINEL ADVANTAGE:** Sentinel's monitoring center is staffed with bilingual personnel on every shift in order to ensure successful interactions with its agency customers. Sentinel monitoring center personnel typically answer 96% of all calls within eight (8) seconds and provide an on-hold wait time of four (4) seconds or less. All of Sentinel's monitoring center employees undergo a thorough and detailed training and certification program, during which they are trained in all aspects of electronic monitoring equipment and software including troubleshooting and the necessary alarm procedures to ensure timely and accurate notifications. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel monitoring center staff is cross-trained to support assistance requests for radio frequency (RF) electronic monitoring, voice verification monitoring programs, breath alcohol testing (BAT), transdermal alcohol monitoring and **global positioning satellite (GPS) tracking** should any participating agency be utilizing more than one (1) service category. Two (2) full weeks are used during the training of a new monitoring center operator to ensure that a thorough electronic monitoring knowledge based is developed. Complete equipment functionality and software platform protocols must be understood prior to graduation to a Level One Monitoring Center Operator. The training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge- and performance-based, allowing maximum participation by monitoring center staff and supervisors. The training

techniques, tools, and exams are developed by the training coordinator and are required to successfully complete the certification process. The coordinator will conduct training sessions at regularly scheduled intervals; however, each shift supervisor will be instrumental in the development of their employees.

Monitoring Center On-going Training: To maintain an efficient service oriented organization, Sentinel employs on-going training modules for all positions. This method is applied equally to all monitoring center operators as to allow correct interpretation and dissemination of information to all authorized agency personnel. The training modules for each employee within the monitoring center are delineated. Sentinel is committed to providing the highest level of monitoring services in the industry. A critical element of providing reliable and efficient monitoring is a knowledgeable, professional and well-trained staff.

This training and certification manual contains the guidelines, curriculums, job descriptions, and policies necessary for the growth and development of monitoring employees. It is knowledge and performance based, allowing maximum participation by monitoring center staff and supervisors. A grading system has been established to easily identify staff members with certain knowledge and ability. This grading system requires an employee to demonstrate acquired skills through verbal and written examinations.

Levels:

- Monitoring Specialist Level – Trainee
- Monitoring Specialist Level – 1
- Monitoring Specialist Level – 2
- Monitoring Specialist Level – 3
- Monitoring Shift Supervisor

Training / Certification: The Training Coordinator is responsible for developing the training techniques, tools, and exams that are required to successfully complete the certification process. The Training Coordinator will conduct training sessions at regularly scheduled intervals; however each shift supervisor will be instrumental in the development of their employees. Training for the various levels will be conducted as follows:

Level	Training Conducted By	Certified By

Trainee	Training Coordinator	Training Coordinator
1	Shift Supervisor	Training Coordinator
2	Shift Supervisor	Training Coordinator
3	Training Coordinator	Training Coordinator
Shift Supervisor	Monitoring Center Manager	Monitoring Center Manager

Certification Exams: A written examination is prepared for each grade level. Some grade levels require that an employee demonstrate acquired skills. A minimum test score is required to pass the written examination.

Level	Minimum Score
Trainee	85%
1	85%
2	85%
3 / Shift Supervisor	90%

A passing score is mandatory for the Trainee and Level 1 position and is required for continued employment. The Level 1 certification exam must be successfully completed before the expiration of a new employee's orientation period. Re-testing periods are established to give an employee an additional attempt to achieve a passing score.

Level	Testing Period	Re-Testing Period	Passing Score
Trainee	When initial training complete	14 Days	Mandatory
1	10 weeks' employment	14 Days	Mandatory
2	90 Days	30 Days	Not Mandatory
3	90 Days	30 Days	Not Mandatory

A passing score is mandatory for continued employment beyond the orientation period for the Trainee and Level 1 grade.

Promotion: This performance-based program ensures that qualified candidates

are promoted in a manner consistent with Sentinel's goal of maintaining a knowledgeable and professional staff. A staff member will be promoted upon successful completion of the certification process. An employee that meets the length of service requirements for a grade promotion must be recommended for advancement by their supervisor. Supervisors are advised to consider the following items before recommending an employee for promotion.

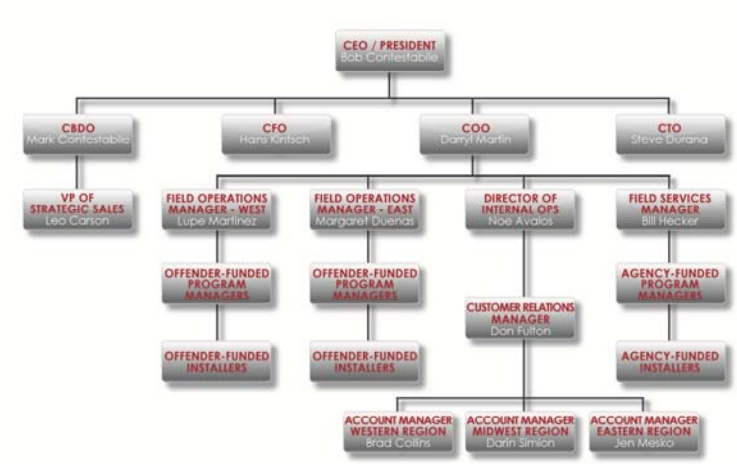
Performance:

- Attendance
- Dependability

Measuring Tools:

- Report
- Charts

Additionally, Sentinel's strong nation-wide presence of qualified field services staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract. The following is a Key Personnel Organizational Chart followed by descriptions of the associated project tasks of Operational Staff responsible for this contract.



Sentinel has a proven track record of providing excellent performance and flexibility to its customers and will commit this same dedication to the Western

			States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all services including but not limited to technical assistance, customer support, inventory, billing and information technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value. **IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness.
9.2	On-Site Service	The Vendor shall provide remote diagnostic support and trouble-shooting technical assistance via a toll-free telephone line 24 hours a day, seven (7) days a week, including holidays. In the event of technical problems that are not resolved from a remote location, the Agency Program Manager, upon request, may require the Vendor to provide on-site, technical assistance within 72 hours.	**Sentinel exceeds this requirement. Staffed customer service and remote diagnostic support through technical support operators are available through a toll-free telephone number, toll-free facsimile and/or email 24 hours a day, seven (7) days a week, 365 days a year at the monitoring center at no additional charge to the participating agencies.** All monitoring services will be provided by Sentinel personnel and equipment. **Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.** **Additionally, each participating agency will be assigned a liaison field services staff member that will be dispatched to provide on-site service in the event of the need for technical assistance, electronic diagnosis or replacement of component problems within 72 hours of requested service.** **IMPORTANT SENTINEL ADVANTANGE: To Sentinel's knowledge, sentinel is the only leading provider of monitoring services that operates two (2) redundant electronic monitoring centers in Irvine, California and Atlanta, Georgia that are staffed and fully operational 24 hours a day.** Sentinel strives to resolve any customer inquiries promptly and on the first contact and the majority of technical problems are resolved through technical telephone support, through remote diagnostics, or through equipment replacement using the on-site spares. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to customer needs such as clearing an alert, changing a participant's schedule, performing participant enrollments or entering data into the system. Operators can also

			provide troubleshooting with tier 1 steps to resolve equipment related issues, monitoring problems or overdues. As an additional enhancement to Sentinel's 24 hour a day support services, during the busiest periods of the day, Sentinel provides an additional team of support staff delivering specialized services to customers. This specialized support services department includes tier 2 advanced troubleshooting for resolving hardware and software issues for all products and services supported by Sentinel. As a result, during the busiest periods of the day the specialized support services team provides added support services including accessing software platforms for user set up, establishing agency notification protocols, equipment inventory, orders and returns. In addition, this specialized support services department performs testing and triage of critical or on-going events to the appropriate department(s) for resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify and mitigate re-occurrence of issues that affect Sentinel customers. This department also assists in researching issues to determine the root cause, provides written resolutions to customers, participates in user acceptance testing and round table discussions for product development enhancements, and serves as a secondary point of contact to the Account Management/Field Services personnel for customer enhancement requests, suggestions and ideas.
9.3	Litigation-Related Testimony	The Vendor shall 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 the Agency. The Vendor shall immediately notify the Agency GPS Program or designee upon receipt of any subpoena involving or affecting the Agency.	**Sentinel meets this requirement.** Sentinel understands the required testimony obligations, and Sentinel is fully prepared to provide qualified personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports while under oath in a court of law. Should the need occur for testimony in court upon request of the participating agency and/or in response to a subpoena, Sentinel will provide expert court testimony, either in person or written witnesses qualified to defend the integrity of Sentinel systems and services. Sentinel, with 20 years proven experience, has maintained integrity and credibility with numerous courts throughout the country on behalf of the agencies it serves. Sentinel will be able to submit the monitoring documentation as supporting evidence when describing the program participant's activities while on GPS tracking. Sentinel will immediately notify the participating agency GPS Program Manager or designee upon receipt of any subpoena involving or affecting the agency. Additionally, Sentinel request advance written notice from the agency of the need for such testimony if possible.

			IMPORTANT SENTINEL ADVANTAGE: On a daily basis Sentinel has as many as **50 employees a day working in court rooms** nationwide testifying regarding participant activity. **This level of experience is difficult to replicate by any vendor and Sentinel is confident that its proposed program can exceed the court's expectations.**
9.4	Quality Assurance Program	The Vendor shall have a formal quality assurance/quality control program in place that demonstrates that internal review and quality control processes are in place and routine evaluations of the quality of the system, equipment and service are performed to ensure compliance with the terms and conditions of the Contract.	**Sentinel exceeds this requirement.** Sentinel has implemented a fully established internal quality assurance/quality control plan addressing all core business operations to demonstrate its willingness to be held accountable for the success of this program. Routine evaluations of the quality of the system, equipment and services are performed to ensure compliance with the terms and conditions of the contract. **Sentinel believes this plan has been successful in making Sentinel programs a success and will follow this plan to measure Sentinel's performance and delivery of services if selected for award.** Sentinel confirms that it has a formal quality control program in place for all department and has attained ISO 9001:2008 certification for manufacturing and Electronic Monitoring Services. Sentinel Offender Services, LLC has implemented processes that have a direct impact to continuous improvement in its Quality Management System. Sentinel's Quality Management System includes the implementation of ISO approved policies and procedures in an effort to achieve the highest possible level of standardization and quality business practice. Sentinel's systems are regularly tested and reviewed to ensure optimum performance standards are met. The tests include all aspects of Sentinel's services, not just functional performance test and monitoring equipment evaluation. Additionally, the results are thoroughly documented, including how cases are being managed and equipment is being issued to participants. Upon contract award, Sentinel will review and modify its Quality Control Plan with WSCA and its participating agencies as needed. Sentinel is in a unique position as it stands ready with fully trained, currently employed personnel to provide a full transition and mobilization of this project.
9.5	Monitoring and Evaluation Requirements	The Agency Program Manager or designated staff may perform Agreement compliance reviews during the term of the Agreement. The Agency Program Manager may include periodic review of compliance with contract service	**Sentinel exceeds this requirement.** Sentinel understands that any participating agency Program Manager or designated staff may perform agreement compliance reviews during the term of the contract including periodic reviews of compliance with contract service delivery. Should issues of non-compliance are identified in any written compliance reports submitted to Sentinel, Sentinel will perform an internal review evaluation of the specific non-compliance and the applicable

		delivery. The Agency Program Manager will provide written compliance reports to the Contractor. When issues of non-compliance are identified, a written Corrective Action Plan (CAP) will be required of the Vendor. The CAP is to be submitted to the Agency Program Manager within ten (10) days of receipt of the Agreement compliance review report. Failure to correct deficiencies after thirty (30) days from the date of receipt of the written Agreement compliance review report notating the deficiencies may result in determination of breach of contract and termination of services.	Standard Operating Procedures. Upon completion of the internal reviews, the Quality Assurance Specialist will ensure the review is sent to the Director of Internal Operations, Chief Operating Officer and appropriate management staff. Management staff will thoroughly discuss the review with any applicable employees to ensure any concerns are appropriately addressed. A Corrective Action Plan will be created and contain notations to summarize the deficiency and be used to document the outcome of the review process. The Corrective Action Plan will be signed by any applicable employee(s) and manager. The Corrective Action Plan will be developed to set clear and realistic goals to correct any deficiencies and enhance the professional development of any reviewed employee. This Corrective Action Plan shall specify, in writing, the corrective measures to be taken with timeframes for resolution included. All Corrective Action Plans will be provided to customers as they are completed, but not more than 10 days of receipt of any compliance review report noting deficiencies. Areas of concern will be reviewed with customer during scheduled quarterly meetings or as requested. Sentinel understands that failure to correct deficiencies after 30 days from the date of receipt of the written agreement compliance review report notating the deficiencies may result in determination of breach of contract and termination of services. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel has established standards that serve as minimum performance criteria throughout the company. These standards will not be enforced as contradictory to the orders of any customers but, rather, to ensure that Sentinel manages the offender monitoring process to the highest possible level of consistent professionalism possible. The Quality Management Team will routinely revise company standards as needed and publish these revisions through memos, emails, checklists and SOP changes. These company standards, regardless of the medium employed for communicating them, will be adhered to as the minimum standards for Sentinel and will be effective immediately as indicated. Along with these Universal Standards a series of checklists and Key Performance Indicator Reports will be available to employees in all department and/or at offices for purposes of self-evaluating their compliance with standards both applicable to the company as well as their department/office. Where local differences may exist between the Universal Standards and the local standards, the highest possible standard that does not conflict with the local courts/agencies will be observed.

			IMPORTANT SENTINEL ADVANTAGE: The Chief Operations Officer requires corrective action plans are developed should any **EXTERNAL OR INTERNAL REVIEW** result in deficiencies and follow-up is implemented in each office or department to ensure timely completion of the plan. The Quality Assurance Specialist or designee will address any deficiency in these areas with managerial staff to ensure appropriate action items are listed and followed through. Upon implementation of a corrective action plan, department supervisors and direct responsibility employees meet regularly as determined by the deliverable timelines to ensure that each Key Performance Indicator is successfully achieved. Sentinel conducts these reviews until it is determined that all milestone achievement markers have been fully fulfilled and the overall corrective goal is accomplished ensuring Sentinel quality standards are maintained.
9.6	Performance Measures Requirements	The Vendor shall ensure that the below stated performance outcomes and level of achievement are met during the term of the Contract:	**Sentinel exceeds this requirement.** Sentinel has implemented a fully established internal quality assurance/quality control plan addressing all core business operations to demonstrate its willingness to be held accountable for the success of this program. Routine evaluations of the quality of the system, equipment and services are performed to ensure compliance with the terms and conditions of the contract. **Sentinel believes this plan has been successful in making Sentinel programs a success and will follow this plan to measure Sentinel's performance and delivery of services if selected for award.** Sentinel confirms that it has a formal quality control program in place for all department and has attained ISO 9001:2008 certification for manufacturing and Electronic Monitoring Services. Sentinel Offender Services, LLC has implemented processes that have a direct impact to continuous improvement in its Quality Management System. Sentinel's Quality Management System includes the implementation of ISO approved policies and procedures in an effort to achieve the highest possible level of standardization and quality business practice. Sentinel's systems are regularly tested and reviewed to ensure optimum performance standards are met. The tests include all aspects of Sentinel's services, not just functional performance test and monitoring equipment evaluation. Additionally, the results are thoroughly documented, including how cases are being managed and equipment is being issued to participants.

			Sentinel is highly experienced in the effective management of this program through its current incumbent radio frequency electronic monitoring program, which provides **a better understanding of the participating agencies' overall monitoring needs than any other vendor in the industry**. Sentinel believes that an expanded partnership with the Western States Contracting Alliance for the **lease of alcohol and GPS monitoring options** not currently available to the department will develop this into a world-class program similar to other programs in the nation and regionally provided through Sentinel. Upon contract award, Sentinel will review and modify this plan with WSCA and its participating agencies as needed. Sentinel is in a unique position as it stands ready with fully trained, currently employed personnel to provide a full transition and mobilization of this project.
9.7	Performance Measures Requirements	a. Ninety-five percent (95%) of all required reports shall be timely submitted.	**Sentinel meets this requirement.** Sentinel is presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program regarding reports in particular. Sentinel is willing and open to discussion with the Western States Contracting Alliance and its participating agencies regarding any of the presented standards and will revise these standards to meet the requirements of the agencies as agreed upon.

Performance Outcomes and Standards Report

Standard	Maximum Allowable Degree of Deviation from Requirement (AQL)\	Measure	Actual
Reports			
All reports are submitted timely	Late required reports not to exceed 5% of the number of required reports	Monthly	
All reports are submitted are accurate	Inaccurate reports required reports not to exceed 5% of the number of required reports	Monthly	
Corrective Action Planning			
Timely submission of Corrective Action Plans	Any required Corrective Action Plan must be submitted within 10 days of receipt of request 100% of the time	Occurrence and Annual	
Timely delivery of requirement under Corrective Action Plans	All required Correction Action Plan deliverables must be submitted completely and by the required due date 100% of the time	Occurrence and Annual	

9.8	Performance Measures Requirements	b. Ninety percent (90%) of training evaluation forms completed on the Vendor's training sessions shall indicate a score of satisfactory or better.	**Sentinel meets this requirement.** Sentinel is presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program regarding training in particular. Sentinel is willing and open to discussion with the Western States Contracting Alliance and its participating agencies regarding any of the presented standards and will revise these standards to meet the requirements of the agencies as agreed upon.

Performance Outcomes and Standards Report

Standard	Maximum Allowable Degree of Deviation from Requirement (AQL)\	Measure	Actual
Timeliness			
Training Delivered Prior to Contract Implementation	100% of all training sessions must be completed prior to the contract implementation date.	Occurrence	
Delivery			
Fully Trained User Agency staff	Training evaluations must indicate training was satisfactorily delivered by at least 90% of trainees for each training session	Occurrence	
Corrective Action Planning			
Timely submission of Corrective Action Plans	Any required Corrective Action Plan must be submitted within 10 days of receipt of request 100% of the time	Occurrence and Annual	
Timely delivery of requirement under Corrective Action Plans	All required Correction Action Plan deliverables must be submitted completely and by the required due date 100% of the time	Occurrence and Annual	

9.9	Performance Measures Requirements	c. Ninety percent (90%) of officer's, supervisors and Manager evaluation forms completed on the Vendor's hardware, system software, monitoring center services and overall customer support shall indicate a score of satisfactory or better.	**Sentinel meets this requirement.** Sentinel conducts customer satisfaction surveys of every customer on a quarterly basis specifically addressing the effectiveness of the hardware, system software, monitoring center services and overall customer support. Sentinel institute a departmental Corrective Action Plan should 90% of survey indicate a score less than satisfactory or better in any category. Sentinel is also presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program regarding manager evaluations in particular.

			Additionally, Sentinel monitors its performance for monitoring center services and overall customer support. Sentinel is presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program regarding monitoring center services and overall customer support. Sentinel is willing and open to discussion with the Western States Contracting Alliance and its participating agencies regarding any of the presented standards and will revise these standards to meet the requirements of the agencies as agreed upon.

Performance Outcomes and Standards Report

Standard	Maximum Allowable Degree of Deviation from Requirement (AQL)\	Measure	Actual
Customer/Technical Support			
Zero monitoring staff errors	Number not to exceed 1% of active units during any 30 day period	Monthly	
Inbound telephone calls promptly answered	95% of inbound calls answered within 30 seconds during each 30 day time period	Monthly	
Inquiries/Complaints unresolved after 5 working days	Number not to exceed 1% of active units during any 30 day period	Monthly	
Corrective Action Planning			
Timely submission of Corrective Action Plans	Any required Corrective Action Plan must be submitted within 10 days of receipt of request 100% of the time	Occurrence and Annual	
Timely delivery of requirement under Corrective Action Plans	All required Correction Action Plan deliverables must be submitted completely and by the required due date 100% of the time	Occurrence and Annual	
Other Contractual Requirements			
Other contractual requirements on a per contract basis	100% compliance with all contractual requirement not otherwise listed	Quarterly	

9.10	Performance Measures Requirements	d. One hundred percent (100%) of system failures shall be reported to	**Sentinel meets this requirement.** Sentinel believes disaster recovery is extremely important to its successful operations and the integrity of its programs

		the Agency within thirty (30) minutes of occurrence.	within the corrections industry and therefore maintains a formal Disaster Recovery Plan. Each member of Sentinel's staff is trained on the execution of the plan and their role is constantly reviewed to promote efficiency of execution. Sentinel regularly monitors key performance indicators for system failure, reporting of system failures, schedule downtime, unscheduled downtime, reporting of downtime and error rates for calls to ensure maximum system performance. Additionally, Sentinel performs regularly scheduled disaster recovery tests to build in a level of quality assurance that is maintained as Sentinel grows as a successful business. To support operations for database replication of key IT, and failover disaster recovery, Sentinel's monitoring system incorporates redundant Disaster Recovery Plan (DRP) servers. While Sentinel's primary monitoring center is located in California, its back-up monitoring center and DRP servers are located in Atlanta, Georgia, over 500 miles apart. The backup DRP facility has state-of-the-art redundant power backed by enterprise level UPS (for short term power loss) and also backed by generators in case of long term power outage. As such, Sentinel offers full (100%) on-site and full (100%) off-site redundancy with fault tolerant central computer systems that guarantee 99.96% uptime performance to receive, store and disseminate data from the field. This redundant system ensures that all services are continuously maintained should a major disruption occur to the primary system, providing a fully resilient and redundant, on-line failover solution to minimize dependence on backups. Should a period of failover occur, there will be no interruption in participant monitoring and no data lost from the monitoring units because data is stored until it is successfully transferred. Sentinel is presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program system failures in particular. Sentinel is willing and open to discussion with the Western States Contracting Alliance and its participating agencies regarding any of the presented standards and will revise these standards to meet the requirements of the agencies as agreed upon.

Performance Outcomes and Standards Report

Standard	Maximum Allowable Degree of Deviation from Requirement (AQL)\	Measure	Actual
System Up-time			
System Failure and implementation of a disaster recovery plan	System Failure and implementation of a disaster recovery plan	System Failure and implementa-tion of a disaster recovery plan	
Reporting System Failure within 30 minutes of occurrence	Reporting of system failure to the User Agency within 30 minutes of occurrence 100% of the time	Occurrence	
Scheduled Monitoring System Downtime	Scheduled downtime not to exceed one (1) hour in a calendar month. No downtime scheduled outside of the hours of 9 am to noon, Monday through Friday.	Monthly	
Unscheduled Downtime	Total unscheduled downtime does not exceed four (4) hours in any calendar month. Single event downtime does not exceed 1 hour within any 30 day period	Monthly	
Reporting of Unscheduled Downtime within 30 minutes of occurrence	Reporting of unscheduled downtime to customers within 30 minutes of occurrence 100% of the time	Occurrence	
Error Rate for Call-Failure	Number not to exceed 5%	Monthly	
Corrective Action Planning			
Timely submission of Corrective Action Plans	Any required Corrective Action Plan must be submitted within 10 days of receipt of request 100% of the time	Occurrence and Annual	

9.11	Performance Measures Requirements	e. One hundred percent (100%) of monthly usage charges shall be invoiced to the Agency within 15 days after the end of the month service is provided.	**Sentinel meets this requirement.** Sentinel is presenting the following program specific Key Performance Indicators (KPIs) that Sentinel believes are essential to any effective electronic monitoring program billing in particular. Sentinel is willing and open to discussion with the Western States Contracting Alliance and its participating agencies regarding any of the presented standards and will revise these standards to meet the requirements of the agencies as agreed upon.

Performance Outcomes and Standards Report

Standard	Maximum Allowable Degree of Deviation from Requirement (AQL)\	Measure	Actual
Accuracy of Billing for Agencies			
All Agencies-Funded Contracts are Being Invoiced	Invoices are not being sent to 1% of agency-funded contracts in any 30 day period	Monthly	
Accuracy of Billing for Participants			
All Offender-Funded Contracts are Being Invoiced	Invoices are not being sent to 1% of participant-funded contracts in any 30 day period	Monthly	
Demographic Information			
Billing Address are Accurate in the Billing System	Invoices are being returned to sender by 0.5% of billed agencies/participants in any 30 day period	Monthly	
Custom Invoice Requirements are Maintained in Billing System	Invoices are being rejected for payment by 0.5% of agency customers due to invoice requirements not being met	Monthly	
Monitoring Rates and Fees			
Invoices Contain Correct Monitoring Rates	Invoices are being rejected for payment by 0.5% of agency customers due to incorrect monitoring fees being accessed in any 30 day period	Monthly	
Invoices Contain Correct Fees	1% of contracts are incorrectly being accessed (rejected for payment) or NOT accessed fees (uncollected income) per contract terms in any 30 day period	Monthly	
Invoiced Days			
Invoices	0% of contracts are incorrectly	Annually	

9.12	Performance Measures Requirements	The Vendor shall advise the Agency, in writing, of any extenuating circumstances that will prohibit the Vendor from meeting the above-outlined performance measures. The Vendor shall provide quarterly performance plan reports to the Agency Program Manager.	**Sentinel meets this requirement.** Any findings by Sentinel's Quality Management Team that require urgent attention or extenuating circumstances that will prohibit Sentinel from meeting the above-outlined performance measures will be prioritized and communicated to the customers **immediately**, in writing, though the appropriate Project Director or Manager. **Quarterly, Sentinel will provide any customer a summary Quality Assurance Report, as requested. This report will detail all findings and identify any trends in operational activities.** All Corrective Action Plans will be provided to customers as they are completed, if they are requested. Areas of concern will be reviewed with customer during scheduled quarterly meetings and a revised, prioritized Corrective Action Plan will be established, if needed. All of Sentinel's Quality Assurance Reports and office/field audits will be available to customers during the execution and close out of projects, if requested.
9.13	Background Checks	The Vendor shall conduct Criminal background checks for security purposes on all of its employees designated as GPS tracking and monitoring staff. The results of the background checks shall be available for review by the Agency. The MCC Contract Administrator on behalf of the Agency has full discretion to require the Vendor to disqualify, prevent, or remove any of its staff from any work being performed under the Contract upon the report of an unsatisfactory background check.	**Sentinel meets this requirement.** Sentinel understands the importance of having qualified, capable, and trustworthy personnel to handle the needs of a program of this complexity where services are provided to an ethnically, racially, chronologically (age), and economically diversified participant population. Therefore, **Sentinel performs a USIS Widescreen National Criminal/Sex Offender search, state specific misdemeanor and felony checks based on addresses received from their personal Experian TRAC report by social security number, and five-panel drug-testing on its employees before hiring.** Sentinel has in place a company-wide drug-free policy that is clearly outlined prior to hiring with Sentinel as well as clearly posted in common work areas. All employees prior to hiring are subjected to a drug screening, and Sentinel conducts random testing based on reasonable cause. **These results of background checks and/or drug tests can be provided to the agency upon request.** Sentinel understands that Contract Administrator on behalf of the WSCA participating agencies has full discretion to require the awarded vendor to disqualify, prevent, or remove any of its staff from any work being performed under the contract upon the report of an unsatisfactory background check.
9.14	Background Checks	The Vendor shall not offer employment to any individual or assign any individual to work under this Contract, who has not had a background check, conducted and the findings of the background check have been determined to be satisfactory.	**Sentinel meets this requirement.** Sentinel's review process ensures that the candidates meet all background, educational, and experience standards as set forth by contractual obligations. In the event of a misdemeanor, Sentinel can provide a release for the employee to provide permission to release the necessary information to the state regarding the specifics of the employee's event. **Sentinel does not hire persons with felony convictions, misdemeanors with moral turpitude, or individuals who have not had a background check**. All of Sentinel's employees are thoroughly screened to ensure that its employees' backgrounds can be verified and that they can be trusted with access to

			corrections facilities, court offices, and confidential offender and agency records. **Only authorized personnel have access to offender data, and Sentinel monitoring center personnel are not allowed to modify any monitoring data without proper authorization from participating agency. At no time will Sentinel ever disclose confidential data to any unauthorized personnel without written approval of the participating agency and all program data will be maintained in accordance with secure data protection standards.** The only staff members who will receive information on program participants are personnel that are assigned to this program's operations and no information is disclosed by these staff members to any third party without written authorization of the participating agency. Each employee is required to acknowledge and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements may result in the possible termination of Sentinel's employees. All records created for defendants referred to this program will remain the property of the participating agency. Upon completion of services, all records will be returned to the participating agency or destroyed under direction of agency authorized personnel. Additionally upon hiring, all Sentinel employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. Sentinel will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.
10.0	**SECTION J Additional Vendor's Equipment and Services**		
Item	**Function**	**Description**	**Describe how Vendor meets or exceeds specifications**

10.1		The Vendor may offer additional Equipment and Services. The Vendor should provide list and include a summary of each additional piece of equipment, to include: one device or system devices, description, training manuals, functionality, service, and optional pricing. Services may be negotiated based on each user Agency's needs.	**Sentinel has proposed the following Optional / Additional Satellite Monitoring and Remote Tracking Service (One-piece Body-attached Device Monitoring Services:** **Optional Uni-Trak™ Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device:** Sentinel proposes Optional Uni-Trak™ as an optional/additional form of Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device. Sentinel's UniTrak one-piece GPS unit provides agencies with added confidence that with no hand-held unit to carry, the participant can no longer 'forget' to bring their tracking device with them as sometimes happens with traditional two-piece GPS tracking systems. The UniTrak device is a small, lightweight one-piece GPS tracking unit. The unit is designed to operate under normal atmospheric conditions and temperatures and the device's enclosure is manufactured with high impact, hypo-allergenic plastic that is 100% water and moisture proof and shock resistant to ensure participant safety and health while still providing consistent tracking capabilities. This design also allows a participant to conduct all normal daily activities, including showering, without affecting the UniTrak's operation. The UniTrak features a lithium-ion rechargeable battery that has a battery-life of 12 months and provides more than 30+ hours of continuous tracking service. It also offers three (3) built-in LED indicator lights, vibration motors for participant alert purposes. **IMPORTANT SENTINEL ADVANTAGE: UniTrak meets the WSCA requirements for Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device. The following list highlights some of the unique features of the proposed UniTrak one-piece GPS:** ▪ **Location-Based Services and/or AFLT:** As an **Alternate Tracking Solution** from possible loss of GPS signal reception, this is the latest in tracking technology that uses cellular tower triangulation to determine a participant's location. This is a key factor for ensuring continuous

			tracking of participants at all times. This application is ideal for situations where the unit is in motion but GPS is not being acquired as this allows us to continue securely tracking the program participant. ▪ **USB Charging Port:** The UniTrak features a USB-port-style for faster and uninterrupted charging. ▪ **Multiple Call-In Frequency Options:** As an industry standard, the reporting frequency will be to collect a point per minute with download every tenth minutes. As a new feature and advantage to Sentinel customers, this reporting frequency can be adjusted to fit different population needs that may equate in to a more frequent or less frequent, downloading format. ▪ **Tamper Alert Strap:** The UniTrak is equipped with an anti-tamper feature to ensure program participants remain securely monitored for the duration of their time on the program. The UniTrak provides accurate GPS tracking through up to 12 satellites, giving it better GPS acquisition and more accurate data than the competition. This high-capacity reception allows for a more accurate determination of the participant's location to within a 50 foot radius, under optimal conditions. Other GPS tracking devices have smaller receiver capabilities that may affect the accuracy of individual point identification due to the inability to connect with the required number of satellites to successfully configure a tracking point. The UniTrak also features the latest in dual-tamper alert technology including severing of the strap or the removal of the strap and backplate from the device. The design incorporates a secure locking mechanism that cannot be unlocked or removed without leaving "tell-tale" signs of the tamper efforts of the participant. The snap-and-lock installation requires no tools as the strap is secured between the backplate and the UniTrak and locked in place when the unit is snapped on the participant's ankle. The UniTrak is designed to overcome tamper attempts in a variety of ways. Once the UniTrak is properly installed on the participant's ankle, the UniTrak cannot be removed unless the strap is cut or severed, thereby compromising the strap and generating a tamper alert. If the participant attempts to pry open or remove the UniTrak unit itself from the strap, a tamper alarm will also be generated.

			IMPORTANT SENTINEL ADVANTAGE: Perhaps the most important benefit is that the UniTrak one-piece GPS unit does not have to rely on cellular service at the residence for home supervision due to the use of an optional redundant home monitoring unit. This design allows for the use of Sentinel's **"Redundant GPS over RF"** tracking and monitoring model with the UniTrak's non-commercially available radio frequency signals emitted over multiple bandwidths allowing the signals to be received by an optional **partnered** beacon or home monitoring unit without interference, replication or duplication. The radio frequency monitoring provided at the residence with the optional beacon or home unit **eliminate GPS drift point issues and ensures real-time residential monitoring**. Sentinel is the only vendor that has tethered its one-piece GPS unit to a true home monitoring unit as an option. Unlike some vendors who merely offer a low, medium, or high range setting, Sentinel's home monitoring equipment offers range settings that are **adjustable for up to 400 feet or down to smaller than 50 feet**, depending on the size of the participant's living arrangements. **Upon entering the residence, the home monitoring unit assumes the monitoring of the participant through proven radio frequency enabled design.** The UniTrak unit functions with Sentinel's home-based receiver unit to perform standard house arrest radio frequency monitoring without relying on GPS to confirm the participant's residential curfew compliance. Upon exiting the residence, the home monitoring unit reports the participant's exit and the UniTrak resumes automatically collecting and reporting GPS locations back to the Sentinel monitoring center via its built-in cellular capability. This advanced and combined, GPS and RF design eliminates officers having to waste valuable time reviewing or investigating false exit alerts created by drift that might be created with other systems that do not have this feature. **IMPORTANT SENTINEL ADVANTAGE:** For recharging purposes, the Sentinel UniTrak GPS unit is charged with a six (6) foot charging cable via USB connection. Based on the same proven technology as the TrakMate II, the UniTrak offers flexible tracking levels (Active, Hybrid and Passive) in a convenient ankle-worn unit. **The levels of service are built-in to the software and do not require Sentinel staff or agency staff to "change out" or replace equipment in order to change a participant's level of GPS supervision.**

			Each time the UniTrak communicates with the monitoring center, it reports its unique serial number for participant identification and all tracking data with a date- and time-stamp. For communication with the monitoring center, the UniTrak utilizes the CDMA cellular network. Additionally, The UniTrak GPS tracking device is equipped with internal memory and internal clock to store any tracking data that is not relayed to the monitoring center for any reason with a date and time stamp. Each device can indefinitely store points in its internal memory so that if the unit cannot relay the data via the cellular networks for any reason, once communication is restored, all tracking points will be downloaded to the system for processing. Based on the level of tracking selected, the appropriate alarms and violations are processed in near real-time format for near immediate notification. All levels of tracking allow authorized staff (Sentinel and agency) to set **inclusion and exclusion zones** to restrict participants' movements around the community. Staff may modify the zones as needed at anytime through the SenTrak website. All alarms will be automatically processed by the monitoring software based on the level of tracking. Based on agency requirements, all alarms will be processed within the required timeframes and notifications are sent as required to any electronic messaging enabled system (text, email, etc.) or direct officer contact.
11.0	**SECTION K Vendor Provided Offender Services**		
Item	**Description**		**Describe how Vendor meets or exceeds specifications**
11.1	The Vendor may offer, Offender Funded/Full Service Programs. The Vendor shall provide locally based staff to implement this program and may recoup the costs for their services directly from the offender. Services may be negotiated based on each user Agency's needs and may include any/all of the following: • Offender Enrollment • Offender Initial Contact • Installing of Devices on Offender • Monitoring of Offender with Initial Investigation of Alerts with Notification to Officer on Verified Violations • Field Service Calls/Maintenance of Equipment • Offender orientation, fee assessment and collection of fees from Offender • Case Management Services • Work/school verification		**Sentinel exceeds this requirement.** Sentinel's current service spectrum provides service options to distinct offender popul provides electronic monitoring, GPS tracking and programs that entail compliance to court orders, ar department and/or the court through both an agenc offender-funded model. **Offender Funded Programs:** Sentinel has always been an innovator in its industry and **in fact pioneered the offender-funded program model** in response to changing industry needs.

	• Schedule entry/maintenance • Collateral office visits to review compliance, adjust schedules.	Sentinel understands that the objectives of offender-funded programs are to provide accountability to the participants through provision of selected court-referred programs and **ensuring each adult, with a demonstrated ability to pay, is responsible for payment for his and/or electronic monitoring**. Additionally, this model allows Sentinel to provide all of its monitoring services at little or no cost to the agencies, **thereby saving correctional agencies tens-of-millions-of-dollars in jail cost and monitoring fee avoidance**. Offender-funded electronic monitoring is Sentinel's core business operation and with no impact on operational budgets to fund these monitoring programs, agencies were able to further expand the programs without requiring additional funds to pay for monitoring services. Currently, Sentinel provides collection of fees from defendants and daily reporting to the court, **specifically for more than 45,000 offender-paid participants.** Sentinel **has monitored more than 1 million offender-paid electronic monitoring participants**. **Sentinel has placed more offenders through offender-funded programs than the rest of the monitoring industry combined**. Through the use of a network of field offices and centralized collections efforts, Sentinel has directly collected **more than $35 million** in fees, fines, and restitution and has additionally remitted funds back to agencies or victims at no additional charge to its customers. When enrolling a participant onto monitoring services, Sentinel will access the ability of the participant to pay for his or her monitoring and services. Sentinel is proposing the implementation of a sliding fee schedule, which allows for the assessment of a daily participation fee based on the participant's overall "ability to pay" to reimburse the costs, or a portion of the costs, of providing supervision. The financial assessment conducted by Sentinel will include, but shall not be limited to, consideration of all of the following factors: (1) Present financial position. (2) Reasonably discernible future financial position to pay in the next six months from the date of acceptance into the program for purposes of determining reasonably discernible future financial position. (3) Likelihood that the person shall be able to obtain employment within the six-month period from the date of acceptance into the program. (4) Any other factor that may bear upon the person's financial capability to reimburse the county for the fees fixed pursuant to subdivision.

IMPORTANT SENTINEL ADVANTAGE: As previously stated, Sentinel pioneered the concept of offender-funded services and is highly experienced in incorporating a sliding fee scale model including the provision of services to participants that are deemed indigent should an agency choose to utilize this model.

Sentinel's experience with offender-paid programs indicates that some level of payment for service, regardless of the amount, is a strong enhancement in the performance of the participant in the program, resulting in a substantial reduction in recidivism. Sentinel has the ability to offer a graduated fee scale available to the WSCA participating agencies for determination of reduced fees to be collected for an indigent participating offender where some participants will be able to pay the full program fees while some will only be able to pay a portion of the daily fees or no fees at all. As part Sentinel's offender-funded program,

Sentinel will collect fees from participants on a flat fee or sliding scale basis based on the following Offender Funded Program on the following characteristics:

- Minimum average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
  - ✓ Initial activation/orientation
  - ✓ Equipment return
  - ✓ Offender-fee payments
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variances with any WSCA end user agency for Offender Funded Program Services.

Sentinel has a current financial assessment form already in use at other various agencies as well as proven invoicing and fee collections procedures in place to ensure program success right out of the gait should any agency choose to utilize these services. The methodology used by Sentinel for determining offender-funded fees is based on Sentinel's extensive experience, performance and success in providing these services to other criminal justice entities.

For those participants that show inability to pay full program fees after all the above elements have been considered, Sentinel will offer a discounted rate off of the full program fees to the participant. The rate will be based on an assessment of the participant's ability to pay. Should the participant not agree with the assessment and discounted rate, Sentinel will provide its finding to the participating agency/courts for recommendations on how to proceed. Sentinel understands that no offender can be denied access to the program based on their inability to pay. **Sentinel will use the following strategies to ensure successful collections:**

- Sentinel local staff will address the importance of keeping current with all program fees and each participant will be required to sign an agreement which outlines program fees and how and when program fees are to be submitted.
- Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc.

- **IMPORTANT SENTINEL ADVANTAGE:** Sentinel will also offer an

		optional on-site Kiosk that will allow offenders to pay monitoring fees electronically. **PLEASE NOTE:** Through this kiosk, Sentinel can offer an optional service to allow offenders to pay other fees owed to the participating agency or other county/city/state agencies such as parking tickets, court fines or restitution. ▪ Prior to any scheduled field or office visit, program staff will review the participant's payment status and any amount that is delinquent. If delinquent, this will be reviewed with the offender to determine the reason. ▪ Sentinel local staff will promptly follow-up on missed or partial payments. ▪ Sentinel will reassess the financial conditions for those participants who have experienced a sudden change in income in order to reevaluate if the participant's ability or inability to pay the established and agreed upon program fees warrant a reduction in fees. ▪ Sentinel will use collection agencies if needed in order to recoup established program fees. ▪ Sentinel will provide monthly reports to the participating agency and/or courts that provide details on fees collected from the offender funded program. ▪ Sentinel will also provide a report that will detail Sentinel's efforts for collecting fees from delinquent participants. ▪ Sentinel will immediately advise the participating agency and/or courts on any offender's refusal to pay program fees to see about having the participant removed from the program. **Sentinel will be responsible for invoicing and the collection of fees from all participants.** Participants may pay for program costs and fees by certified checks, money orders and credit cards. It will be preferred at the time of installation that the participant provides a credit or debit card for ease and compliance which has been proven to increase collection rates and decrease court assisted collection measures. However, should a participant be unable to provide a credit or debit card, to enhance the collection of offender payments, Sentinel will offer follow-up call-center intervention to remind offenders of over-due payments and to arrange payments as needed. Sentinel's Collections Call Center operates during non-conventional business hours so that Sentinel can contact offenders when they return home from employment, school, treatment, etc. **IMPORTANT SENTINEL ADVANTAGE:** All participant payments made to

Sentinel are processed through Sentinel's proprietary SenTrack software and made available to the participating agencies or courts via this automated software interface and in hard copy reports/invoices. Within this system, Sentinel will track the progress of participant payments as well as alcohol test results, drug screens, report dates, and other court order conditions that may be required by or beyond the Scope of Work for this program. All activity is automatically time- and date-stamped within the software for chronological integrity purposes. SenTrack allows Sentinel to manage both the case management aspects and financial aspects of the defendant case through one (1) software program that is web-accessible and can be interfaced with the participating agencies case management software.

Full Service Programs: Sentinel is proposing several value-added options to help elevate the burden of routine program management, installation/retrieval service, compliance monitoring, inventory management and fee collections from WSCA participating agency employees allowing officers more time to manage violations and provide needed case management to its offender population. Sentinel provides options for both **limited or full-service case management** in addition to installation and retrieval services will allow both agencies to simply refer participants to Sentinel and receive violation notifications for all program participants through immediate automated or manual notifications.

Sentinel's installation and retrieval, limited- and/or full-case management programs include on-site Sentinel staff to ensure each participant meets all the terms of his and/or her sentence, including electronic sup fees, fines, and restitution, and counseling or treatment, w

Case supervision services are an integral component of the judicial process; therefore selecting the correct service provider is a critical decision. **Sentinel currently provides case management services to more than 100 programs from more than 50 locally-based offices across the country.** In these programs, Sentinel's staff monitors compliance to the court-ordered conditions with court orders via regularly scheduled meetings with each participant,

addresses all issues of non-compliance, and reports continued non-compliance to the supervising agencies for resolution. Sentinel maintains individual case files on all participants for review by the court or its designees and in order to provide documentation for use in enforcement or revocation matters. Additionally, Sentinel has extensive experience customizing programs at the local level and currently **works directly with over 95 judges**.

Through these programs, Sentinel's supervision services staff conducts more than **55,000 face-to-face defendant contacts a month**. Additionally, Sentinel understands the importance of expert court testimony and on a daily basis Sentinel has as many as **50 employees a day working in court rooms** nationwide testifying regarding participant activity. **This level of experience is difficult to replicate by any vendor and Sentinel is confident that its proposed program can exceed the court's expectations.**

Sentinel's case management model would allow for a full time office to be opened and local staff to be hired and trained. Once established this location could be utilized by participating agencies for programs like offender paid drug testing, cognitive skills courses and job readiness programs. The ability to expand your programs to include new and innovative solutions is paramount to long term success and the reduction in participant recidivism rates. Sentinel has extensive experience provide the following staff members to programs utilizing its limited- or full-service case management services:

Program Director: Dependent on the size of the specific program, Sentinel may employ a Program Director as the lead contact for the daily operation of the program and handle any court requests. The candidate will hold at minimum a Bachelor's Degree in social work or counseling and have counseling or social work experience with participants. This person's duties will include:

- Daily reconciliation of all payments received
- Supervision of all Sentinel office staff
- Quality assurance audits and reviews of supervision methodologies
- Oversee all contacts with victims
- Investigate all participants grievances
- Daily liaison for court personnel
- Court representative for any proceedings for participants
- Steering committee representative for Sentinel with court/agency personnel

Case Manager(s): Case Manager candidates will also hold at minimum of a Bachelor's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include:

- Adhering to Sentinel's Case Management Model including performing (1) Assessment, (2) Interpretation, (3) Case Planning, (4) Ensuring the Delivery of Services and (5) Evaluating Performance
- Explaining all program rules and expectations to the defendants and obtaining the defendant agreement to the same through signature
- Create and maintain files on all participants referred to the program
- Process all payments
- Communication with court personnel if there are any inquiries on a specific participants
- Perform notifications of program completions/non-compliance

Administrative Assistant: Depending on the size of the specific programs and the volume of tasks placed on an office providing this type of service to a participant population, an Administrative Assistant maybe needed. This person will:

- Handle all calls received at the office
- Provide assistance to the Program Director and Case Manager(s) as needed
- Assist with performing any required transmission of reports
- General office tasks

IMPORTANT SENTINEL ADVANTAGE: Sentinel designed its proprietary, web accessible case management software, SenTrack, specifically for use in the offender services arena. Employing SenTrack allows **real-time, on-line web accessibility** to participant case information and reports for Sentinel employees **and** authorized participant agency and/or court personnel. As the SenTrack case management software is an in-house concept and design, SenTrack is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. **Sentinel is not reliant on an outside vendor for new editions or support and recommends all participating stakeholders have access to the SenTrack software for program review and oversight.**

Sentinel catapulted the speed, capacity and capabilities of case management

software through the development of the SenTrack SQL database system. The SQL database structure is infinitely able to generate reports, elicit statistical data and conduct queries for specific information as needed to meet literally any requirement or report objective. **This translates into the ability to modify or develop new software variations as may be needed for the agency directly, in house, without having to utilize outside vendors which may bring data security concerns to the agency. Only Sentinel personnel would have access to the confidential participant data and the development of any new application.**

Sentinel's SenTrack case management software incorporates all of the technology offered by Sentinel including the Kiosk. The software is fully integrated in every Sentinel branch office and has become the foundation from which Sentinel serves its customers. Highlights of the SenTrack case management software include:

- Internet accessibility; available 24 hours a day to any Sentinel customer
- All client obligations to the court are tracked (courses, fines, drug screens, community service, restitution, demographics etc.)
- Real-time communication with Kiosks
- On-line payment acceptance
- Proprietary Case Management Software; 100% in-house support and customization available
- Over 150 available reports
- Customized reports provided at **no cost**
- Currently services more than 200 agencies and over 45,000 offender-paid participants
- Able to capture photo images as required
- Fully redundant and supported by continuous operation monitoring center designed to Underwriters Laboratory specifications
- Internal audit tools track all changes
- Unlimited query capabilities for detailed statistical reporting

The SenTrack system is completely customizable and currently provides more than 150 different types of case management and financial reports. Through the ability to customize the system, SenTrack has made it possible for judges to have the reports they want in the format they desire.

IMPORTANT SENTINEL ADVANTAGE: Sentinel has helped pioneer the

concept of opening local, community-based "Success Centers" where probationers/defendants/parolees can participate in electronic monitoring programs and optionally receive assistance with job placement, address drug addiction, as well as participate in cognitive skills classes, anger management and other developmental programs. Using this model, Sentinel can work directly with the participating agency and the courts to develop additional programs at its Success Center to help reduce recidivism **AT NO COST TO THE AGENCY**. Sentinel's basic business model rests on proven research that has shown that heavier punishment and long terms of incarceration or probation are not lasting answers to stem criminal behavior. Rehabilitation-oriented programs and defendant accountability, combined with community-based intervention and support, is the more sensible way to tackle this complex issue.

Should participating agencies elect to utilize the Success Center Model, Sentinel will additionally provide the following staff members:

Program Specialist(s): Program Specialist candidates will hold at minimum a Master's Degree in social work or counseling and have counseling or social work experience with defendants. Job duties include:

- Delivery of daily classes based on Diversion Orders or needs assessments
- Communication with the Project Director/Case Manager(s) regarding each defendants progress regarding his or her Case Plan
- Maintaining current on all applicable laws and changing regulations for class delivery

Sentinel understands that each of the following services may be negotiated based on each participating agency's needs and may include any/all of the following:

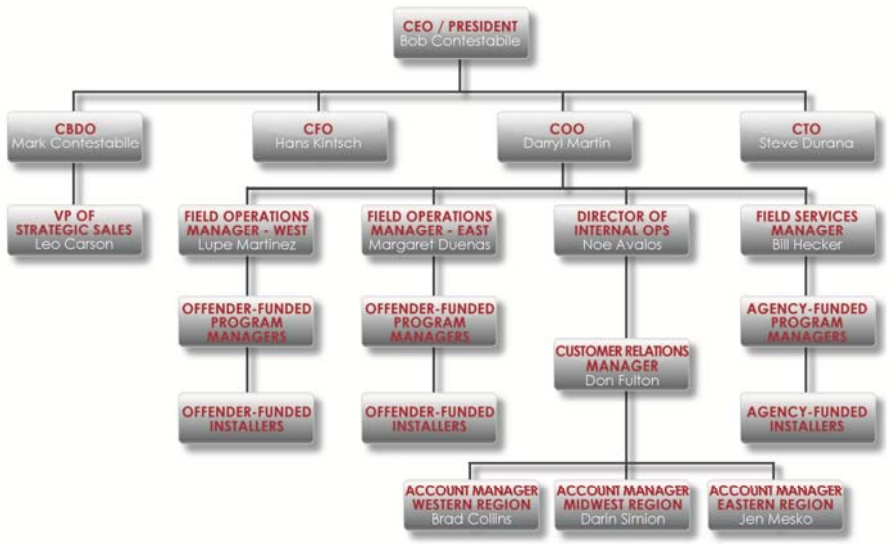
Offender Initial Contact/Enrollment: As part of Sentinel's provision of full service programs, Sentinel utilizes the services of the Sentinel Enrollment Department. This team handle can handle all new enrollment duties with program participants. For this project, they can be the first tier of contact with a defendant **(if not referred to Sentinel's office directly after court)** that would allow us to inform the defendant of all program requirements prior to enrollment in the event that they had any questions. Sentinel's Enrollment Department can assist with new enrollments for these programs when appropriate to ensure

		efficient local office operations. When a participant is referred to the house arrest electronic monitoring program, he or she is expected to report to the program within one (1) business day to begin services but no later than 72 hours from referral. The first time the participant reports to Sentinel's office, the Project Director/Case Manager completes the standard Intake Form and enters the participant's information in SenTrack, Sentinel's unique electronic case management system. During this interview, the Project Director/Case Manager will collect information using Motivational Interviewing techniques which are extremely important during the participant's first encounter with the Project Director/Case Manager. From the moment the participant enters the office, the participant will be made aware that he and/or she is welcomed in the program and that the program exists to help the participant succeed in completing his or her sentence. **Offender Orientation:** Sentinel's Project Director/Case Manager(s) will be responsible for conducting an Intake and Orientation meeting with each program participant to complete all set-up and system requirements with the person sentenced or placed on the electronic monitoring program at the participant's home, place of business or other location(s) as determined by the participating agency/court. The orientation is the most important appointment held with the participant as it sets the parameters of the participant's monitoring and program regulations. Sentinel's Project Director/Case Manager(s) will collect and verify all of the necessary participant documentation and information to verify the participant's employment, community restitution, treatment classes, religious activities, funeral services, medical appointments and any other activities the person participates in on an on-going basis. In addition to confirming the participant's information, all permitted activities and required verification/ documentation including reasons for possible termination from the program would be explained to the participant so that there were no misunderstandings. **Please note:** Sentinel understands it may not terminate any person's participation with the program without first notifying the participating agency/court and receiving correspondence from the participating agency/court giving Sentinel permission to terminate the person from the home detention electronic monitoring program. During this meeting Sentinel will:

		▪ Obtain a copy of the Pre-conviction or conviction from the participant, jail and/or court ▪ Verify participant's name, date of birth, home address, telephone number, race and family details ▪ Verify court details including docket number, assigned judge, date of the court order, anticipated date of execution of sentence and restitution requirements ▪ Capture participant photograph and signature ▪ Obtain signature of participant consent for the Authorization for Information Release (if required) ▪ Complete a financial assessment of the participant to determine indigent status (if required) ▪ Complete a risk/need assessment to determine the participant's Case Plan (if full-service option selected) ▪ Inform the participant of the days they are required to report into the office for face-to-face meetings ▪ Review required restitution and fee payments Another important segment of the Intake and Orientation is the fee payments. Using the approved fee schedules as set forth herein, Sentinel will review the costs of the program as well as any restitution payment requirements, ensure all required payments have been made and receive any payments scheduled at this time. Sentinel Project Director/Case Manager(s) will explain the fee structure and inform the defendant that his or her case will be completion only if he or she complies with the conditions, completes all program requirements and has already paid all restitution owed to the victim and all fees. For either limited or full-service case management models, Sentinel **recommends** that at a minimum the goals for the house arrest electronic monitoring program should include successful completion of court mandated rehabilitation programs including (e.g. domestic violence programs, education classes, GED preparation, life skills training, mental health counseling/treatment, parenting classes, substance abuse counseling/treatment and other classes deemed necessary), timely arrival at all meetings/programs and maintenance of timely payments. **After providing thorough explanations of both the program parameters and the fee structures, Sentinel Project Director/Case Manager(s) will obtain a written agreement from each participant prior to enrollment, indicating the**

		participant agrees with all conditions of the home detention electronic monitoring program. **Installing of Devices on Offender:** During the Intake and/or Orientation meeting, the Project Director/Case Manager(s) will install and activate all necessary electronic monitoring equipment on the participant. Sentinel can offer a full continuum of electronic home monitoring equipment to monitor and verify that program participants remain at home/work during specified time periods and shall report unauthorized absences, late returns, equipment malfunctions, verbal responses and other functions to a central computer system. **Initial Investigation of Alerts with Notification to Officer on Verified Violations:** Sentinel abides by the ideals of providing accurate and timely information and provides several methods of automatic notification for officers immediately or upon expired grace period. Sentinel supports all standard methods of notification, such page (alpha or numeric), electronic mail, fax, and/or text message to a cell phone. **In addition to automated notifications, Sentinel is highly experienced at providing triage services via monitoring center staff whereby live operators will make a manual voice call to any combination of officer's office/mobile phones and to participant's mobile and/or home phones for direct voice communications in response to specific alerts.** Most agencies defer initial alerts and equipment related alerts to automated notifications and use manual voice only when necessitated for monitoring center staff intervention on confirmed alerts or when direct communications with a participant is necessitated. . At no additional cost, Sentinel will customize each individual participating agency's notification profiles to include grace periods for specified violations before the system generates notification should the agency request this service. **Field Service:** Sentinel has a proven track record of providing excellent performance and flexibility to its customers and will continue to commit this same dedication to the Western States Contracting Alliance and its participating agencies. Sentinel has assembled a multi-faceted Project Team with a supportive Management Team to provide the participating agencies with all field services including but not limited to on-site technical assistance and 24 hour a day customer support as well as inventory, billing and information

		technology support. The experienced Project Team and Management Team assembled for this project include several staff members that add significant value. **IMPORTANT SENTINEL ADVANTANGE: Leo Carson, Vice President of Strategic Sales has 23+ years of in-depth experience delivering electronic monitoring including 11+ years to the Western States Contracting Alliance.** Mr. Carson will be tasked with assessing the program against the industry best-practices to proposed creative solutions to the agency to enhance effectiveness. Sentinel's extensive depth of field services personnel (as shown on the following organizational chart) will provide corporate oversight for the contractual cycle of each of the participating programs during the program lifecycle. The assigned field services personnel will be dispatched to provide on-site service in the event of the need for electronic diagnosis or replacement of component problems. Field services personnel will also be responsible for scheduling training, per the contract, with agency staff on the use of equipment and reading reports. This strong nation-wide presence of qualified Sentinel staff will ensure that participating agencies needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for this Western States Contracting Alliance contract.



Additionally, staffed monitoring services and technical support are available from Sentinel 24 hours a day, seven (7) days a week, 365 days a year. Sentinel's Engineering Department, in conjunction with its IT staff, is on-call 24 hours a day, seven (7) days a week to support operations, resolve any system issue, and ensure continued operations. **The agency can be confident that Sentinel is experienced and fully capable of providing the necessary transactional, technical and support services on a continuous basis, 24 hours a day, seven (7) days a week, 365 days a year.**

Maintenance: Sentinel is the Original Equipment Manufacturer of the majority of its equipment and systems and confirms that all equipment provided to WSCA participating agencies will be covered by a full manufacturer's warranty **for the length of any contract**. Sentinel will maintain all equipment in good operating condition and free from materials defects and/or workmanship under normal and proper use for the term of this agreement.

Sentinel's warehouse supports the daily operations of all Sentinel electronic monitoring programs. Based in Southern California, Sentinel's warehouse is responsible for the provision of all equipment nationwide. Sentinel's assigned Account Manager will work proactively with each Western States Contracting Alliance participating agency to ensure the appropriate amount of equipment and

		spares are maintained for the electronic monitoring of offenders. This open communication allows Sentinel to provide equipment in a timely manner without having to depend on costly overnight / express delivery in order to meet the program's equipment needs. In the event of any malfunction of any piece of equipment, Sentinel will provide routine equipment maintenance repair through the return and replacement of malfunctioning equipment at no additional cost to participating agencies. Sentinel will ship all replacement equipment within five (5) business days. Sentinel will provide up to 15% of the actual number of units in use with each individual participating agency as on-site spare equipment for each equipment type selected at each participating agency location **at no charge**. These non-active spare units will be stored locally and allow for **immediate onsite replacements** of equipment on the participant that may become inoperable, lost, stolen or damaged or as additional units in the event of sudden program expansion. This spare shelf stock of equipment ensures there is no delay in services due to the non-availability of equipment. Additionally, if any agency's spare inventory is depleted, Sentinel will re-supply the appropriate equipment via overnight delivery at no additional cost within 24 hours after notification. All shipping costs (both delivery and return) of all equipment and supplies will be the responsibility of Sentinel. **Product Warranty:** Sentinel represents and warrants that, upon delivery of any product and/or consumable to the delivery location, such product will have been manufactured, filled, packaged, stored and shipped materially in accordance with the specifications or custom specifications for such product in accordance with the associated purchase order. Sentinel further represents and warrants that it shall obtain and maintain all necessary licenses, permits or approvals in connection with the manufacture, filling, packing, testing, storage and shipment of each such product. **Sentinel warrants all of its equipment and software for the life of the contract.** This includes software maintenance, licensing and future feature enhancements. **Warranty Service:** Warranty service with Sentinel is a very simple process. The participating agency only needs to contact the proposed Account Manager to discuss warranty service and/or feature upgrades. Sentinel is committed to the continual development of feature enhancement and product development. The Account Manager will also work with the Sentinel training department to provide

		any training required by a new feature or upgrade to the equipment or system. **Work/school Verification:** Sentinel will verify all pre-approved locations including work, school, college, counseling, AA/NA, victim awareness or other program classes and capture teacher/supervisor information for additional follow-up. **Schedule Entry/Maintenance:** Sentinel Project Director/Case Managers will profile new participant enrollments, perform all schedule entry and schedule management. The electronic monitoring program will continuously monitor participants within their assigned schedules as determined by the participating agencies/courts. When enrolling participants, Sentinel Case Managers will set up curfew information on a per participant basis in the **WEB PATROL II®** software. The **WEB PATROL II®** software supports an unlimited number of curfew/absence periods per client, per day and will allow authorized users to create, edit and delete all parameters for individual participants. **Collateral office visits to review compliance, adjust schedules:** Sentinel understands the importance of having a robust, accountable process to ensure that participants referred into the program are held accountable and are treated fairly and with respect while participating in the program. During regularly scheduled office visits, Project Director(s)/Case Manager(s) will periodically review the participant's file for the duration of the participant's time in the program to review participant compliance, adjust schedules and collect fee(s). The proposed program includes regular check-in and contacts that will allow the participant the ability to show accountability and proactively advance through the program. It has been proven that regular check-ins in the early program stages and throughout the program have led to more successful outcomes. **IMPORTANT SENTINEL ADVANTAGE:** Sentinel services include the incorporation of the latest technological advancements in the defendant services arena including Sentinel's Kiosk check-in and reporting capabilities, Sentinel's latest electronic monitoring equipment and formalized collections programs. All of these tools and technologies can be incorporated in the provision of WSCA participating agency programs including multi-level supervision and fees determined by the defendant's case requirements.

APPENDIX E PRICE SHEETS

Daily is defined as 12:00 AM to 11:59:59 PM. Pricing shall be the not to exceed pricing on a per product/service basis.

CATEGORY 1 – RADIO FREQUENCY (RF) ELECTRONIC MONITORING

Description		Qty	Unit	Daily Rate*
Radio Frequency (RF) Continuous Signaling Electronic Monitoring Service (Receiver (Home Unit) - Landline Communication Connection)	**Equipment/Unit (when in use)**	1 - 100	EA	$1.00
		101 – 250	EA	$1.00
Body-Attached Ankle Bracelet (transmitter):		251 – 500	EA	$1.00
Mfg.: Sentinel Offender Services, LLC		501 – 1,500	EA	$1.00
Brand/Model: RF Patrol®		1,501 – 3,000	EA	$1.00
With **Receiver/Home Unit** with Landline Connection:		3,001+	EA	$1.00
Mfg.: Sentinel Offender Services, LLC				
Brand/Model: RF Patrol®	**Monitoring Service/Unit (when in use)**	1 - 100	EA	$0.91
		101 – 250	EA	$0.84
		251 – 500	EA	$0.78
		501 – 1,500	EA	$0.74
		1,501 – 3,000	EA	$0.69
(*Daily rate determined on a per customer basis.)		3,001+	EA	$0.66

Description		Qty	Unit	Daily Rate*
Radio Frequency (RF) Continuous Signaling Electronic Monitoring Service (Receiver (Home Unit) - Cellular Communication Connection)	**Equipment/Unit (when in use)**	1 - 100	EA	$2.00
		101 – 250	EA	$2.00
		251 – 500	EA	$2.00
Body-Attached Ankle Bracelet (transmitter):		501 – 1,500	EA	$2.00
Mfg.: Sentinel Offender Services, LLC		1,501 – 3,000	EA	$2.00
Brand/Model: RF Patrol® Cellular		3,001+	EA	$2.00
With **Receiver/Home Unit** with Cellular Communication:	**Monitoring Service/Unit (when in use)**	1 - 100	EA	$0.91
Mfg.: Sentinel Offender Services, LLC		101 – 250	EA	$0.84
Brand/Model: RF Patrol® Cellular		251 – 500	EA	$0.78
		501 – 1,500	EA	$0.74
		1,501 – 3,000	EA	$0.69
(*Daily rate determined on a per customer basis.)		3,001+	EA	$0.66

Description	Unit	Unit Price
Lost/Damaged/Stolen Equipment Replacement for above RF Continuous Signaling Electronic Monitoring Equipment		
Body-Attached Ankle Bracelet Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol®	EA	$250.00
Receiver (Home Unit) – with Landline communication connection. Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol®	EA	$500.00
Receiver (Home Unit) – with Cellular communication. Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol® Cellular	EA	$800.00

Description	Qty	Unit	Daily Rate*
Preferred Optional Service: Radio Frequency (RF) Random/Scheduled Tracking Service			
Equipment/Unit (when in use)	1 - 100	EA	$N/A
Voice Patrol ® Does NOT require participant equipment	101 – 250	EA	$N/A
Mfg.: Sentinel Offender Services, LLC	251 – 500	EA	$N/A
Brand/Model: Voice Patrol®	501 - 1000	EA	$N/A
	1001 +	EA	$N/A
Monitoring Service/Unit (when in use)	1 +	EA	$1.75
(Includes 5 contacts/participant/day per 10.7			
(*Daily rate determined on a per customer basis.)			

Description	Order Qty	Unit	Unit Price
Preferred Optional Service: Radio Frequency (RF) Mobile (Drive By) Receiver **Equipment/Unit** Mfg.: Sentinel Offender Services, LLC Brand/Model: RF Patrol® Drive-By	101 +	EA	$1.00 Daily Rate

Optional Service: Radio Frequency (RF) Electronic Monitoring Service – Optional Vendor Provided Offender Services

Vendor may offer and provide Radio Frequency (RF) Monitoring Service on an optional basis for both juvenile and adult Participants to Agencies operating on a local or statewide basis. Vendor shall provide staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Vendor's administrative fee to administer (including invoicing services) and provide an optional Offender Funded Program shall be an additional $Included per unit/day. (No Cost to the End User Agency) – For Offender Funded Radio Frequency (RF) Services, Sentinel will collect fees from participants on a flat fee or sliding scale basis at the rate of approximately 1 to 1.5 times the participant's hourly wage, per day in the program based on the following Offender Funded Program on the following characteristics:

- Minimum, average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
  - Initial activation/orientation
  - Equipment return
  - Offender-fee payment
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variance with any WSCA end user agency for Offender Funded Program Services.

Vendor shall provide staff to implement this program and may recover the costs for their services at a negotiated amount directly from the Agency and or Participant.

Description of Optional Services	Typical Daily Charge
1. Optional Sentinel Kiosk for Random/Scheduled Tracking, Reporting, Offender Fee Collections	$75.60/unit/day
2. Optional Sentinel Kiosk for Random/Scheduled Tracking, Reporting, Offender Fee Collections	$Sliding Scale/unit/day

Optional Radio Frequency (RF) Monitoring Services	Qty	Unit	Daily Rate*
Optional Alert Notifications (Reference Specifications. 5.0)			
1. Closed-loop Notification (notify with confirmation of Officer call-back verification)	1	EA	$Included
2. Escalating notification (notify, pause for call-back verification, escalate to notify next Officer/contact, pause, continue)	1	EA	$Included
Curfew and equipment status optional alerts reports other than by web-based system and/or email (Ref. Spec. 5.1 – 5.11)			
1. By Fax	1	EA	$Included
2. And/or by telephone	1	EA	$Included
Verbal notification made by Monitoring Center staff to agency personnel or offenders on an optional basis (Reference Specifications. 5.12). Pricing is on a "per call" basis.	1	EA	$Included

APPENDIX E PRICE SHEETS

Daily is defined as 12:00 AM to 11:59:59 PM. Pricing shall be the not to exceed pricing on a per product/service basis.

CATEGORY 2 – ALCOHOL MONITORING EQUIPMENT AND SERVICE

Description	Qty	Unit	Daily Rate*
Alcohol Monitoring Equipment and Service **Equipment/Unit (when in use)**	1 - 50	EA	$2.00
(Receiver (Home Unit) - Landline)	51 – 150	EA	$2.00
	151 – 300	EA	$2.00
Mfg.: Sentinel Offender Services, LLC	301+	EA	$2.00
Brand/Model: MEMS3000 (aka 3M™ Remote Alcohol Monitoring System)			
Monitoring Service/Unit (when in use)	1 - 50	EA	$1.17
	51 – 150	EA	$1.12
Basic Monitoring Service (24x7 help desk and automated alert notification is included in the equipment/unit above	151 – 300	EA	$1.04
(*Daily rate determined on a per customer basis.)	301+	EA	$0.95

Description	Qty	Unit	Daily Rate*
Alcohol Monitoring Equipment and Service **Equipment/Unit (when in use)**	1 - 50	EA	$2.50
(Receiver (Home Unit) - Cellular)	51 – 150	EA	$2.50
	151 – 300	EA	$2.50
Mfg.: Sentinel Offender Services, LLC	301+	EA	$2.50
Brand/Model: MEMS3000 Cellular (aka 3M™ Remote Alcohol Monitoring System)			
Monitoring Service/Unit (when in use)	1 - 50	EA	$1.71
	51 – 150	EA	$1.67
	151 – 300	EA	$1.54
(*Daily rate determined on a per customer basis.)	301+	EA	$1.40

Description	Unit	Unit Price
Alcohol Monitoring Equipment and Service **Lost/Damaged/Stolen Equipment Replacement for above Alcohol Monitoring Equipment**		
Receiver (Home Unit) – Landline Mfg.: 3M Electronic Monitoring Brand/Model: MEMS (aka 3M™ Remote Alcohol Monitoring System)	EA	$1,100.00

Receiver (Home Unit) – Cellular Mfg.: 3M Electronic Monitoring Brand/Model: MEMS3000 Cellular (aka3M™ Remote Alcohol Monitoring System)	EA	$1,350.00

Optional Service: Alcohol Monitoring Equipment and Service – Optional Vendor Provided Offender Services

Vendor may offer and provide an offender funded program for Alcohol Monitoring Equipment and Service. Vendor shall provide staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Vendor's administrative fee to administer (including invoicing services) and provide an optional Offender Funded Program shall be an additional $Included per unit/day. (No Cost to the End User Agency) – For Offender Funded Alcohol Monitoring Services. Sentinel will collect fees from participants on a flat fee or sliding scale basis at the rate of approximately 1.5 to 2 times the participant's hourly wage, per day in the program for Standalone Offender Funder Alcohol Monitoring Services, or a flat additional fee of $5.00/unit/day when used in combination with another WSCA Offender Funded Service, based on the following Offender Funded Program on the following characteristics:

- Minimum, average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
  - Initial activation/orientation
  - Equipment return
  - Offender-fee payment
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variance with any WSCA end user agency for Offender Funded Program Services.

Vendor shall provide staff to implement this program and may recover the costs for their services at a negotiated amount directly from the Agency and or Participant.

Description	Daily Rate*
Alcohol Monitoring Equipment and Service – Optional Services	
Description of Optional Services:	
1. Optional VI-CAP Patrol™ Alcohol Monitoring (Price includes Equipment & Monitoring Services)	$3.92
2. Lost/Damaged/Stolen Equipment Replacement for Optional VI-CAP Patrol™ Alcohol Monitoring Equipment: Camera: $800.00, Tester: $500.00	
3. Optional VI-CAP Patrol™ Mobile, Cellular Alcohol Monitoring (Price includes Equipment & Monitoring Services) Price includes Equipment & Monitoring Services)	$6.50
4. Lost/Damaged/Stolen Equipment Replacement for Optional VI-CAP Patrol™ Mobile, Cellular Alcohol Monitoring Equipment: Device: $500.00	

CATEGORY 2 – ALCOHOL MONITORING TRANSDERMAL EQUIPMENT AND SERVICE

Description		Qty	Unit	Daily Rate*
Alcohol Monitoring Transdermal Equipment and Service	**Equipment/Unit (when in use)**	1 - 50	EA	$3.00
(Receiver (Home Unit) - Landline Communication Connection)		51 – 150	EA	$3.00
		151 – 300	EA	$3.00
Body-Attached Device:		301+	EA	$3.00
Mfg.: Alcohol Monitoring Systems, Inc.				
Brand/Model: SCRAMx	**Monitoring Service/Unit (when in use)**	1 - 50	EA	$4.49
With **Receiver/Home Unit** with Landline Connection: Product Bid:		51 – 150	EA	$4.44
Mfg.: Alcohol Monitoring Systems, Inc.		151 – 300	EA	$4.38
Brand/Model: SCRAMx		301+	EA	$3.89
(*Daily rate determined on a per customer basis.)				

Description		Qty	Unit	Daily Rate*
Alcohol Monitoring Transdermal Equipment and Service	**Equipment/Unit (when in use)**	1 - 50	EA	$4.00
(Receiver (Home Unit) - Cellular Communication Connection)		51 – 150	EA	$4.00
Body-Attached Device:		151 – 300	EA	$4.00
Mfg.: Alcohol Monitoring System, Inc.		301+	EA	$4.00
Brand/Model: SCRAMx Cellular				
With **Receiver/Home Unit** with Cellular Connection: Product Bid	**Monitoring Service/Unit (when in use):**	1 - 50	EA	$4.74
Mfg.: Alcohol Monitoring System, Inc.		51 – 150	EA	$4.69
Brand/Model: SCRAMx Cellular		151 – 300	EA	$4.63
(*Daily rate determined on a per customer basis.)		301+	EA	$4.34

Description	Unit	Unit Price
Required: Lost/Damaged/Stolen Equipment Replacement for above single body-worn device for Alcohol Monitoring Transdermal Equipment and Service		
Body-Attached Bracelet Device for Transdermal Alcohol Monitoring: Mfg.: Alcohol Monitoring Systems, Inc. Brand/Model: SCRAMx	EA	$600.00

Receiver (Home Unit) – Landline Mfg.: Alcohol Monitoring System, Inc. Brand/Model: SCRAMx	EA	$900.00
Receiver (Home Unit) – Cellular Mfg.: Alcohol Monitoring System, Inc. Brand/Model: SCRAMx Cellular	EA	$700.00

Optional Service: Alcohol Monitoring Equipment and Service – Optional Vendor Provided Offender Services

Vendor may offer and provide an offender funded program for Alcohol Monitoring Equipment and Service. Vendor shall provide staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Vendor's administrative fee to administer (including invoicing services) and provide an optional Offender Funded Program shall be an additional $Included per unit/day. (No Cost to the End User Agency) – For Offender Funded Transdermal Alcohol Monitoring Services. Sentinel will collect fees from participants on a flat fee or sliding scale basis at the rate of approximately 2 times the participant's hourly wage, per day in the program for Standalone Offender Funder Transdermal Alcohol Monitoring Services, or a flat additional fee of $6.50/unit/day when used in combination with another WSCA Offender Funded Service, based on the following Offender Funded Program on the following characteristics:

- Minimum, average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
  - Initial activation/orientation
  - Equipment return
  - Offender-fee payment
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variance with any WSCA end user agency for Offender Funded Program Services.

Vendor shall provide staff to implement this program and may recover the costs for their services at a negotiated amount directly from the Agency and/or Participant.

Description of Optional Services	**Typical Daily Charge**
1. Drug Screening – 5 Panel, observed screens, minimum 750 screens per month	$22.00/screen

Description	Daily Rate*
Alcohol Monitoring Transdermal Equipment and Service – Optional Services	
Description of Optional Services: 1. Optional CAM Patrol Plus™ Transdermal Alcohol Monitoring (Price includes Equipment & Monitoring Services) 2. Lost/Damaged/Stolen Equipment Replacement for Optional CAM Patrol Plus™ Transdermal Alcohol Monitoring Equipment: Bracelet: $500.00, Tester: $800.00	$8.74

APPENDIX E PRICE SHEETS

CATEGORY 3 – SATELLITE MONITORING AND REMOTE TRACKING SERVICE (GLOBAL POSITIONING SYSTEM (GPS)) Using One-piece Body-attached Device

Description	Qty	Unit	Daily Rate*
Satellite Monitoring and Remote Tracking Service (One-piece Body-attached Device) – Active, Hybrid and Passive Mode. **Equipment/Unit (when in use):**	1 - 100	EA	$2.00
	101 – 250	EA	$2.00
One-piece Body-attached Device:	251 – 500	EA	$2.00
Mfg.: Omnilink system, Inc.	501 – 1,500	EA	$2.00
Brand/Model: OM Series	1,501 – 3,000	EA	$2.00
(Includes additional accessory (beacon/similar device) for in-home use when needed at no additional cost.)	3,001+	EA	$2.00
Monitoring Service for Active Mode/Unit (when in use):	1 - 100	EA	$1.68
	101 – 250	EA	$1.58
	251 – 500	EA	$1.54
	501 – 1,500	EA	$1.48
	1,501 – 3,000	EA	$1.41
	3,001+	EA	$1.41
Monitoring Service for Required Hybrid Mode/Unit (when in use):	1 - 100	EA	$1.63
(Reference Specifications Sections 4a.13 and 4a.16)	101 – 250	EA	$1.53
This pricing also applies to the vendor's own Optional Hybrid Mode program. Contact vendor for details.	251 – 500	EA	$1.49
	501 – 1,500	EA	$1.43
	1,501 – 3,000	EA	$1.36
	3,001+	EA	$1.36
Monitoring Service for Passive Mode/Unit (when in use):	1 - 100	EA	$1.44
	101 – 250	EA	$1.38
	251 – 500	EA	$1.34
	501 – 1,500	EA	$1.24
(*Daily rate determined on a per customer basis.)	1,501 – 3,000	EA	$1.14
	3,001+	EA	$1.14

Description	Unit	Unit Price
Required: Lost/Damaged/Stolen Equipment Replacement for above one-piece body-attached device for Satellite Monitoring and Remote Tracking Service		
Body-attached Bracelet Device Mfg.: Omnilink Systems, Inc, Brand/Model: OM Series	EA	$500.00
Accessory (such as beacon or similar device) for enhanced location verification and landline communication at home. Mfg.: Omnilink Systems, Inc. Brand/Model: OM Series	EA	$250.00

Optional Service: Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device – Optional Vendor Provided Offender Services

Vendor may offer and provide Satellite Monitoring and Remote Tracking Service on a preferred optional service basis for both juvenile and adult Participants to Agencies operating on a local or statewide basis. Vendor shall provide staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Vendor's administrative fee to administer (including invoicing services) and provide a preferred optional Offender Funded Program shall be an additional $ Included per unit/day (No Cost to the End User Agency) – For Offender Funded GPS 1-Piece Services. Sentinel will collect fees from participants on a flat fee or sliding scale basis at the rate of approximately 2 times the participant's hourly wage, per day in the program based on the following Offender Funded Program on the following characteristics:

- Minimum, average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
    - Initial activation/orientation
    - Equipment return
    - Offender-fee payment
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variance with any WSCA end user agency for Offender Funded Program Services.

Vendor shall provide staff to implement this program and may recover the costs for their services at a negotiated amount directly from the Agency and or Participant.

Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device – Optional Services	Daily Rate*
Description of Optional Services:	
1. Optional Uni-Trak™ Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device (Prices include Equipment & Monitoring Services): Active:	$3.68
Hybrid:	$3.63
Passive:	$3.44
2. Optional Landline Reporting (for Optional Uni-Trak™ Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device (Prices include Equipment & Monitoring Services):	$0.35
3. Lost/Damaged/Stolen Equipment Replacement for Optional Uni-Trak™ Satellite Monitoring and Remote Tracking Service for One-piece Body-attached Device Monitoring Equipment: Bracelet: $500.00, Home Unit: $800.00	
4. Optional Mobile Victim Zone Domestic Violence Program (Price includes dual Offender & Victim OM Series GPS devices with enhanced Monitoring Center triage and law enforcement notification – Price may be negotiated based on each program's unique needs.	$22.00

CATEGORY 3 – SATELLITE MONITORING AND REMOTE TRACKING SERVICE (GLOBAL POSITIONING SYSTEM (GPS)) Using Multi-Piece System

Description	Qty	Unit	Daily Rate*
Satellite Monitoring and Remote Tracking Service (Multi-piece System) – Active, Hybrid and Passive Mode. **Equipment/Unit (when in use):**	1 - 100	EA	$3.00
Body-attached Device: Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II	101 – 250	EA	$3.00
	251 – 500	EA	$3.00
Body-worn Device: Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II	501 – 1,500	EA	$3.00
(Includes additional accessory (beacon/similar device) for in-home use when needed at no additional cost.)	1,501 – 3,000	EA	$3.00
	3,001+	EA	$3.00
Monitoring Service for Active Mode/Unit (when in use):	1 - 100	EA	$1.54
	101 – 250	EA	$1.48
	251 – 500	EA	$1.36
	501 – 1,500	EA	$1.24
	1,501 – 3,000	EA	$1.17
	3,001+	EA	$0.98
Monitoring Service for Required Hybrid Mode/Unit (when in use): (Reference Specifications Sections 4b.13 and 4b.16) This pricing also applies to the vendor's own Optional Hybrid Mode program. Contact vendor for details.	1 - 100	EA	$1.49
	101 – 250	EA	$1.43
	251 – 500	EA	$1.31
	501 – 1,500	EA	$1.19
	1,501 – 3,000	EA	$1.12
	3,001+	EA	$0.93
Monitoring Service for Passive Mode/Unit (when in use):	1 - 100	EA	$1.34
	101 – 250	EA	$1.28
	251 – 500	EA	$1.16
	501 – 1,500	EA	$1.04
	1,501 – 3,000	EA	$0.97
(*Daily rate determined on a per customer basis.)	3,001+	EA	$0.78

Description	Unit	Unit Price
Required: Lost/Damaged/Stolen Equipment Replacement for above multi-piece device system for Satellite Monitoring and Remote Tracking Service		
Body-attached Bracelet Device: Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II	EA	$250.00
Body-worn Device Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II	EA	$500.00
Accessory (such as beacon or similar device) for enhanced location verification and landline communication at home. Mfg.: Sentinel Offender Services, LLC Brand/Model: TrakMate II	EA	$550.00

Optional Service: Satellite Monitoring and Remote Tracking Service for Multi-piece System – Optional Vendor Provided Offender Services

Vendor may offer and provide Satellite Monitoring and Remote Tracking Service on a preferred optional service basis for both juvenile and adult Participants to Agencies operating on a local or statewide basis. Vendor shall provide staff to implement this program and may recoup the costs for their services directly from the Agency and/or Participant. Vendor's administrative fee to administer (including invoicing services) and provide a preferred optional Offender Funded Program shall be an additional $ Included per unit/day (No Cost to the End User Agency) – For Offender Funded GPS Multi-Piece Services. Sentinel will collect fees from participants on a flat fee or sliding scale basis at the rate of approximately 2 times the participant's hourly wage, per day in the program based on the following Offender Funded Program on the following characteristics:

- Minimum, average of 100 active participant per installation area
- Average participant term on monitoring of 30 days
- 75 square mile installation area
- One Sentinel Installer/Case Manager per installation area
- Participants maintain a two-week advance payment
- 75% of participants willing to report to local Sentinel office for:
    - Initial activation/orientation
    - Equipment return
    - Offender-fee payment
- Equipment/Monitoring/Notification consistent with that proposed for WSCA
- Fee collections from participants with an average collection term of 30 days with the ability to remove participants from the program at that term for failure to pay and/or non-payment.

Sentinel acknowledges that these factors may vary on a per program basis, thus Sentinel will remain open to discussing these characteristics and, where necessary, renegotiate any particular variance with any WSCA end user agency for Offender Funded Program Services.