Awarded Vendor
0000103874
Sentinel Offender Services, LLC
1290 N. Hancock St., Ste. 103
Anaheim, CA 92807
Icarson@sentineladvantage.com

Telephone No. (888) 843-5590

Price Agreement Number: 40-000-13-00004AD

Price Agreement Amendment No.: Two

Term: July 26, 2013 – December 31, 2020

Ship To:
All State of New Mexico agencies, commissions, institutions, political subdivisions and local public bodies allowed by law.

Invoice:
As Requested at time of order

Procurement Specialist: Vanessa LeBlanc

Telephone No.: (505) 827-0266

Email: Vanessa.LeBlanc@state.nm.us

Title: Electronic Monitoring of Offenders

This Price Agreement Amendment is to be attached to the respective Price Agreement and become a part thereof.

In accordance with Price Agreement provisions, and by mutual agreement of all parties, this Price Agreement is extended from January 1, 2020 to December 31, 2020 at the same price, terms and conditions.

Update Awarded Vendor Address
From:
201 Technology Drive
Irvin CA, 92618

To:
1290 N. Hancock St., Ste. 103
Anaheim, CA 92807

Except as modified by this amendment, the provisions of the Price Agreement shall remain in full force and effect.

Accepted for the State of New Mexico

New Mexico State Purchasing Agent

Date: 10/24/19

Purchasing Division, 1100 St. Francis Drive 87505, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472
State of New Mexico  
General Services Department  
Purchasing Division  

Statewide Price Agreement Amendment

Awarded Vendor  
0000103874  
Sentinel Offender Services, LLC  
201 Technology Drive  
Irvin CA  92618  

Telephone No.  (888) 843-5590

Price Agreement Number: 40-000-13-00004AD

Price Agreement Amendment No.: One

Term: July 26, 2013 – December 31, 2019

Procurement Specialist: Natalie Martinez  
Telephone No.: (505) 827-0251

Ship To:  
All State of New Mexico agencies, commissions, institutions, political subdivisions and local public bodies allowed by law.

Invoice:  
As Requested

Title: Electronic Monitoring of Offenders

This Price Agreement Amendment is to be attached to the respective Price Agreement and become a part thereof.

In accordance with Price Agreement provisions, and by mutual agreement of all parties, this Price Agreement is extended from January 1, 2017 to December 31, 2019 at the same price, terms and conditions.

Except as modified by this amendment, the provisions of the Price Agreement shall remain in full force and effect.

Accepted for the State of New Mexico

New Mexico State Purchasing Agent  

Date: 11/23/16

Purchasing Division, 1100 St. Francis Drive 87505, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472 nm
STATE OF CONNECTICUT
DEPARTMENT OF ADMINISTRATIVE SERVICES
PROCUREMENT DIVISION
165 Capitol Avenue, 5th Floor South
HARTFORD, CT 06106-1659

CONTRACT AWARD NO.:
12PSX0139

Contract Award Date:
3 July 2013

Bid Due Date:
WSCA/NASPO Contract

SUPPLEMENT DATE:
22 August 2016

CONTRACT AWARD SUPPLEMENT #3
IMPORTANT: This is NOT a Purchase Order. DO NOT Produce or Ship without an Agency Purchase Order.

DESCRIPTION:
Electronic Monitoring of Offenders Services

FOR:
All Using State Agencies and Political Subdivisions

TERM OF CONTRACT:
July 3, 2013 through December 31, 2016
Extended through December 31, 2019

AGENCY REQUISITION NUMBER: 805

CHANGE IN STATE CONTRACT VALUE | CHANGE TO DAS-CERTIFIED SMALL BUSINESS CONTRACT VALUE | CHANGE TO OUT OF STATE CONTRACT VALUE | CHANGE TO TOTAL CONTRACT AWARD VALUE
--- | --- | --- | ---
- | - | $4,000,000.00 | $4,000,000.00 - Est.

NOTICE TO CONTRACTORS: This notice is not an order to ship. Purchase Orders against contracts will be furnished by the using agency or agencies on whose behalf the contract is made. INVOICE SHALL BE RENDERED DIRECT TO THE ORDERING AGENCY.

NOTE: Dollar amounts listed next to each contractor are possible award amounts, however, they do not reflect any expected purchase amounts (actual or implied). They are for CHRO use only.

NOTICE TO AGENCIES: A complete explanatory report shall be furnished promptly to the Procurement Manager concerning items delivered and/or services rendered on orders placed against awards listed herein which are found not to comply with the specifications or which are otherwise unsatisfactory from the agency’s viewpoint, as well as failure of the contractor to deliver within a reasonable period of time specified. Please issue orders and process invoices promptly.

CASH DISCOUNTS: Cash discounts, if any, shall be given SPECIAL ATTENTION, but such cash discount shall not be taken unless payment is made within the discount period.

PRICE BASIS: Unless otherwise noted, prices include delivery and transportation charges fully prepaid f.o.b. agency. No extra charge is to be made for packing or packages.

PLEASE NOTE:

- The above mentioned Contract has hereby been extended from 31 December 2016 through 31 December 2019.
- Refer to next page for Contractor Information.
- All terms and conditions not otherwise affected by this supplement remain unchanged and in full force and effect.

DEPARTMENT OF ADMINISTRATIVE SERVICES
By: [Signature] (Original Signature on Document in Procurement Files)
Name: CAROL WILSON
Title: Procurement Director
Date: 22 August 2016
State of New Mexico
General Services Department
Statewide Price Agreement

Awarded Vendor
0000103874
Sentinel Offender Services, LLC
201 Technology Drive
Irvin, CA 92618

Telephone No. (888) 843-5590

Price Agreement Number: 40-000-13-00004AD
Payment Terms: Net 30
F.O.B.: Destination
Delivery: As listed in contract

Procurement Specialist: Mona Espinosa
Telephone No.: (505) 827-0218

Ship To:
All State of New Mexico agencies, commissions, institutions, political subdivisions and local public bodies allowed by law.

Invoice:
As requested

Title: Electronic Monitoring of Offenders

Term: July 26, 2013 thru December 31, 2016

This Price Agreement is made subject to the “terms and conditions” shown on the reverse side of this page, and as indicated in this Price Agreement.

Accepted for the State of New Mexico

[Signature]

New Mexico State Purchasing Agent

Date: 07/25/13

Purchasing Division, 1100 St. Francis Drive, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472 AM
PARTICIPATING ADDENDUM
WSCA-NASPO COOPERATIVE PURCHASING ORGANIZATION
Electronic Monitoring of Offenders
Administered by the State of Washington (hereinafter “Lead State”)

MASTER AGREEMENT/CONTRACT
Washington Contract Number: 00212

Name of Contractor: Sentinel Offender Services, LLC
(herinafter “Contractor”)

And

Name of participating state/entity: NM State Purchasing Division
(herinafter “Participating State/Entity”)

Page 1 of 4

1. Scope: This addendum covers the purchase of electronic monitoring of offenders services through Contracts lead by the State of Washington for use by state agencies and other entities located in the Participating State/Entity authorized by that state's statutes to utilize state/entity contracts with the prior approval of the state's chief procurement official.

2. Participation: Use of specific WSCA-NASPO cooperative contracts by agencies, political subdivisions and other entities (including cooperatives) authorized by an individual state’s statutes to use state/entity contracts are subject to the prior approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. Participating State Modifications or Additions to Master Agreement: The successful vendor will remit to the State of New Mexico Contract Manager an Administrative Fee in the amount of one percent (1%) of all sales for New Mexico State and Local Public Bodies from this contract. Checks should be made payable to the State of New Mexico.

The Administrative Fee is based upon:

- The sales of all parts and equipment;

In accordance with the following schedule:

<table>
<thead>
<tr>
<th>Period End</th>
<th>Report Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 30</td>
<td>October 31</td>
</tr>
<tr>
<td>December 31</td>
<td>January 31</td>
</tr>
<tr>
<td>March 31</td>
<td>April 30</td>
</tr>
<tr>
<td>June 30</td>
<td>July 31</td>
</tr>
</tbody>
</table>

4. [Purposely left blank].

5. Primary Contacts: The primary contact individuals for this participating addendum are as follows (or their named successors):
PARTICIPATING ADDENDUM
WSCA-NASPO COOPERATIVE PURCHASING ORGANIZATION
Electronic Monitoring of Offenders
Administered by the State of Washington (hereinafter “Lead State”)

MASTER AGREEMENT/CONTRACT
Washington Contract Number: 00212

Name of Contractor: Sentinel Offender Services, LLC

(herinafter “Contractor”)

And

Name of participating state/entity: NM State Purchasing Division

(herinafter “Participating State/Entity”)

Lead State:

<table>
<thead>
<tr>
<th>Name:</th>
<th>Robert Paulson, Jr., C.P.M., Contract Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>State of Washington</td>
</tr>
<tr>
<td></td>
<td>Department of Enterprise Services, Master Contracts &amp; Consulting</td>
</tr>
<tr>
<td></td>
<td>PO Box 41411</td>
</tr>
<tr>
<td></td>
<td>Olympia, WA 98504-1411</td>
</tr>
<tr>
<td>Telephone:</td>
<td>(360) 407-9430</td>
</tr>
<tr>
<td>Fax:</td>
<td>(360) 586-2426</td>
</tr>
<tr>
<td>E-Mail:</td>
<td><a href="mailto:robert.paulson@des.wa.gov">robert.paulson@des.wa.gov</a></td>
</tr>
</tbody>
</table>
PARTICIPATING ADDENDUM
WSCA-NASPO COOPERATIVE PURCHASING ORGANIZATION
Electronic Monitoring of Offenders
Administered by the State of Washington (hereinafter “Lead State”)

MASTER AGREEMENT/CONTRACT
Washington Contract Number: 00212

Name of Contractor: Sentinel Offender Services, LLC

(hereinafter “Contractor”)

And

Name of participating state/entity: NM State Purchasing Division

(hereinafter “Participating State/Entity”)

Contractor:

<table>
<thead>
<tr>
<th>Name:</th>
<th>Sentinel Offender Services, LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>201 Technology Drive, Irvin, CA 92618</td>
</tr>
<tr>
<td>Telephone:</td>
<td>(888) 843-5590</td>
</tr>
<tr>
<td>Fax:</td>
<td>(800) 327-1178</td>
</tr>
<tr>
<td>E-Mail:</td>
<td><a href="mailto:leo.carson@senttrak.com">leo.carson@senttrak.com</a></td>
</tr>
</tbody>
</table>

Participating Entity:

<table>
<thead>
<tr>
<th>Name:</th>
<th>NM State Purchasing Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>PO Box 6850, Santa Fe, NM 87502</td>
</tr>
<tr>
<td>Telephone:</td>
<td>(505) 827-0472</td>
</tr>
<tr>
<td>Fax:</td>
<td>(505) 827-2484</td>
</tr>
<tr>
<td>E-Mail:</td>
<td><a href="mailto:Ramona.Espinosa@state.nm.us">Ramona.Espinosa@state.nm.us</a></td>
</tr>
</tbody>
</table>

6. Purchase Order Instructions:
All orders should contain the following (1) Mandatory Language “This order is subject to WSCA-NASPO Contract # 00212 terms, conditions, specifications and pricing.” (2) Your Name, Address, Contact, & Phone-Number. (3) Other program requirements as necessary.

7. Individual Customer:
Each State agency and political subdivision, as a Participating Entity, that purchases electronic monitoring services will be treated as if they were Individual Customers. Except to the extent modified by a Participating Addendum, each agency and political subdivision will be responsible to follow the terms and conditions of the Master Agreement/Contract; and they will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement/Contract. Each agency and political subdivision will be responsible for their own charges, fees, and liabilities. Each agency and political subdivision will have the same rights to any indemnity or to recover any costs allowed in the contract for their purchases. The Contractor will apply the charges to each Participating Entity individually.

This Participating Addendum and the Master Agreement/Contract number 00212 (administered by the State of Washington) together with its exhibits, set forth the entire agreement between the parties with respect to the subject matter of all previous communications, representations or
PARTICIPATING ADDENDUM
WSCA-NASPO COOPERATIVE PURCHASING ORGANIZATION
Electronic Monitoring of Offenders
Administered by the State of Washington (hereinafter “Lead State”)

MASTER AGREEMENT/CONTRACT
Washington Contract Number: 00212

Name of Contractor: Sentinel Offender Services, LLC
(hereinafter “Contractor”)

And

Name of participating state/entity: NM State Purchasing Division
(hereinafter “Participating State/Entity”)

agreements, whether oral or written, with respect to the subject matter hereof. Terms and
conditions inconsistent with, contrary or in addition to the terms and conditions of this
Addendum and the Master Agreement/Contract, together with its exhibits, shall not be added to
or incorporated into this Addendum or the Master Agreement/Contract and its exhibits, by any
subsequent purchase order or otherwise, and any such attempts to add or incorporate such
terms and conditions are hereby rejected. The terms and conditions of this Addendum and the
Master Agreement/Contract and its exhibits shall prevail and govern in the case of any such
inconsistent or additional terms within the Participating State.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution
by both parties below.

<table>
<thead>
<tr>
<th>Participating State/Entity:</th>
<th>Contractor:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM State Purchasing Division</td>
<td>Sentinel Offender Services, LLC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By:</th>
<th>By:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name:</th>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawrence O. Maxwell</td>
<td>Hans Kintsch</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title:</th>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Purchasing Agent</td>
<td>Chief Financial Officer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 26, 2013</td>
</tr>
</tbody>
</table>

[Additional signatures as required by Participating State]
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 .......................................................................... 8
  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
8.0 INFORMATION AND COMMUNICATIONS

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
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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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 WORKMANSHP
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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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 receivable 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

Page 15 of 541
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 Remediing 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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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;
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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:
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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), or 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.

<table>
<thead>
<tr>
<th>To Contractor at:</th>
<th>To MCC at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentinel Offender Services, LLC</td>
<td>State of Washington</td>
</tr>
<tr>
<td></td>
<td>Department of Enterprise Services</td>
</tr>
<tr>
<td></td>
<td>Master Contracts &amp; Consulting</td>
</tr>
<tr>
<td>Attn:</td>
<td>Attn:</td>
</tr>
<tr>
<td>Leo Carson, Vice President of Strategic Sales</td>
<td>MCC Contract Administrator</td>
</tr>
<tr>
<td>201 Technology Drive</td>
<td>Mail: Post Office Box 41411</td>
</tr>
<tr>
<td>Irvine, California 92618</td>
<td>Olympia, Washington 98504-1411</td>
</tr>
<tr>
<td>Street: 1500 Jefferson Street, SE</td>
<td></td>
</tr>
<tr>
<td>Olympia, WA 98501</td>
<td></td>
</tr>
<tr>
<td>Phone: (888) 843-5590</td>
<td>Phone: (360) 407-9430</td>
</tr>
<tr>
<td>Fax: (800) 327-1178</td>
<td>Fax: (360) 586-2426</td>
</tr>
<tr>
<td>E-mail: <a href="mailto:leocarson@senttrak.com">leocarson@senttrak.com</a></td>
<td>E-mail: <a href="mailto:robert.paulson@des.wa.gov">robert.paulson@des.wa.gov</a></td>
</tr>
</tbody>
</table>

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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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: **Contract 00212**

<table>
<thead>
<tr>
<th>Approved (Lead State)</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>State of Washington</td>
<td>Sentinel Offender Services, LLC</td>
</tr>
<tr>
<td>Department of Enterprise Services</td>
<td>201 Technology Drive</td>
</tr>
<tr>
<td>Master Contracts &amp; Consulting</td>
<td>Irvine, California 92618</td>
</tr>
<tr>
<td>1500 Jefferson Street, SE</td>
<td></td>
</tr>
<tr>
<td>Olympia, WA 98501</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s/</td>
<td>6-3-13</td>
<td>/s/</td>
<td>May 3, 2013</td>
</tr>
<tr>
<td>Robert Paulson, Jr., C.P.M.</td>
<td></td>
<td>Hans Kintsch</td>
<td></td>
</tr>
<tr>
<td>Print or Type Name</td>
<td>Print or Type Name</td>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Contract Administrator</td>
<td>Chief Financial Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s/</td>
<td>6-3-13</td>
</tr>
<tr>
<td>Dale Colbert, CPPO</td>
<td></td>
</tr>
<tr>
<td>Print or Type Name</td>
<td></td>
</tr>
<tr>
<td>Unit Manager</td>
<td></td>
</tr>
</tbody>
</table>

Page 33 of 541
### Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s/</td>
<td>6/4/13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christine Warnock, CPPO</td>
<td>Chief Procurement Officer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance</td>
<td>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.</td>
</tr>
<tr>
<td>Acceptance Testing</td>
<td>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.</td>
</tr>
<tr>
<td>Agency</td>
<td>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. &quot;Agency&quot; does not include the legislature.</td>
</tr>
<tr>
<td>All or Nothing</td>
<td>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.</td>
</tr>
<tr>
<td>Alternate</td>
<td>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.</td>
</tr>
<tr>
<td>Amendment</td>
<td>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.</td>
</tr>
<tr>
<td>Authorized Representative</td>
<td>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.</td>
</tr>
<tr>
<td>Bid</td>
<td>A sealed written offer to perform a Contract to provide materials, supplies, services, and/or equipment in reply to an Invitation For Bid (IFB).</td>
</tr>
<tr>
<td>Bidder</td>
<td>A Vendor who submits a Bid or Proposal in reply to a Solicitation.</td>
</tr>
<tr>
<td>Business Days</td>
<td>Monday through Friday, 8:00 a.m. to 5:00 p.m., Pacific Time, except for holidays observed by the state of Washington.</td>
</tr>
<tr>
<td>Calendar Days</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Contract</strong></td>
<td>An agreement, or mutual assent, between two or more competent parties with the elements of the agreement being offer, acceptance, and consideration.</td>
</tr>
<tr>
<td><strong>Contract Administrator</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Contractor</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Equal</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Estimated Useful Life</strong></td>
<td>The estimated time from the date of acquisition to the date of replacement or disposal, determined in any reasonable manner.</td>
</tr>
<tr>
<td><strong>Inspection</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Invitation For Bid (IFB)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Lead Time/After Receipt Of Order (ARO)</strong></td>
<td>The period of time between when the Contractor receives the order and the Purchaser receives the materials, supplies, equipment, or services order.</td>
</tr>
<tr>
<td><strong>Life Cycle Cost</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Master Contracts &amp; Consulting (MCC)</strong></td>
<td>The MCC within the Washington Department of Enterprise Services, Master Contracts &amp; 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.</td>
</tr>
<tr>
<td><strong>Order Document</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Procurement Coordinator</strong></td>
<td>The individual authorized by the MCC who is responsible for conducting a specific Solicitation.</td>
</tr>
<tr>
<td><strong>Product</strong></td>
<td>Materials, supplies, services, and/or equipment provided under the terms and conditions of this Contract.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Proposal</strong></td>
<td>A sealed written offer to perform a Contract to supply materials, supplies, services, and/or equipment in reply to a Request For Proposal (RFP).</td>
</tr>
<tr>
<td><strong>Purchaser</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Recycled Material</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Recycled Content Product</strong></td>
<td>A product containing recycled material.</td>
</tr>
<tr>
<td><strong>Request For Proposal (RFP)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Responsible</strong></td>
<td>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:</td>
</tr>
<tr>
<td><strong>Responsive</strong></td>
<td>A Bid or Proposal that meets all material terms of the Solicitation document.</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>A Bid or Proposal</td>
</tr>
<tr>
<td><strong>Solicitation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The State of Washington acting by and through the MCC.</td>
</tr>
</tbody>
</table>
| **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 affect 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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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:
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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.senttrak.com](http://www.senttrak.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@senttrak.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@senttrak.com  
   Internet address for company catalog: [www.senttrak.com](http://www.senttrak.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@senttrak.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.
**SPECIFICATIONS**

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

<table>
<thead>
<tr>
<th>CATEGORY 1—RADIO FREQUENCY (RF) CONTINUOUS SIGNALING ELECTRONIC MONITORING SERVICE</th>
<th>SECTION A. Vendor Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>1.1</td>
<td>Vendor Requirements</td>
</tr>
</tbody>
</table>
| 1.2 | Vendor Requirements | Sentinel exceeds this requirement. Sentinel is capable of performing expert on-site 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 ADVANTAGE:** 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 expeditiously, 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.
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Facility</td>
<td>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.</td>
<td>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</td>
</tr>
</tbody>
</table>
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.

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.

<table>
<thead>
<tr>
<th>2.2</th>
<th>Facility</th>
<th>The Vendor shall provide a secure confidential monitoring service center and help-desk facility that provides service 24/7/365.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 confidentiality, 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.
| 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 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 superviser’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-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 (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 ADVANTAGE: 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.

<table>
<thead>
<tr>
<th>2.7</th>
<th>Facility</th>
<th>Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.8</td>
<td>Facility</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

| 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® PHMU’s 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 |
| 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 Symetrax 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 occurs 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 arise. |
**Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders**

<table>
<thead>
<tr>
<th>2.12 Facility</th>
<th>The Vendor’s Monitoring Center should have ventilation and temperature controls adequate to ensure proper functions of the Monitoring Center hardware.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.13 Facility</td>
<td>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.</td>
</tr>
</tbody>
</table>

**back-up monitoring center should any continuous commercial power outage occur that jeopardizes monitoring center operations.**

**IMPORTANT SENTINEL ADVANTAGE:** 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 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.

**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 supervisory 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
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.15</td>
<td>Data Center</td>
<td>The Vendor’s Data Centers must have ventilation and temperature control adequate to ensure proper functions of the Data Center hardware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Sentinel meets this requirement.</strong> 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.</td>
</tr>
<tr>
<td>2.16</td>
<td>Data Center</td>
<td>The Vendor’s Data Centers must have back-up emergency power generators.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Sentinel exceeds this requirement.</strong> 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%</td>
</tr>
</tbody>
</table>
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
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 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. |
| 2.18 | Data Center | All back-up systems in the Data Centers must be tested regularly. | 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. **Sentinel exceeds this requirement.** Sentinel has 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. |
| 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 affects 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 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.

<p>| 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. <strong>Sentinel meets this requirement.</strong> 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: <strong>Sentinel meets this requirement.</strong> The computer system, through SenTrak, immediately and automatically (in real-time) records 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. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.22</td>
<td>a. All historical data must be centrally stored and accessible for reporting purposes; <strong>Sentinel meets this requirement.</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>b. This information must be available for reporting in a standard transaction file format; and <strong>Sentinel exceeds this requirement.</strong> 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.</td>
</tr>
<tr>
<td>2.24</td>
<td>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. <strong>Sentinel exceeds this requirement.</strong> 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.</td>
</tr>
</tbody>
</table>
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 settings 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.

<table>
<thead>
<tr>
<th>2.25</th>
<th>Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**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 re-establishment 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 effect 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 and 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.
<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 2.26    | Data Storage | 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.  
**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. |
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.

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 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:
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

- 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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

<table>
<thead>
<tr>
<th>2.30</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Sentinel meets this requirement.</strong> 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 from the Internet to ensure the remote connection is not compromised. <strong>Personnel Security:</strong> 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</td>
</tr>
</tbody>
</table>

Page 83 of 541
| 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.
| 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. | 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. ** 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Monitoring Center Staff</td>
<td>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:</td>
<td><strong>Sentinel exceeds this requirement.</strong> 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</td>
</tr>
</tbody>
</table>
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 and Sentinel, via its acquisition of G4S Justice Services LLC, has been the incumbentWSCA 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:

<table>
<thead>
<tr>
<th>Level</th>
<th>Training Conducted By</th>
<th>Certified By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trainee</td>
<td>Training Coordinator</td>
<td>Training Coordinator</td>
</tr>
<tr>
<td>1</td>
<td>Shift Supervisor</td>
<td>Training Coordinator</td>
</tr>
<tr>
<td>2</td>
<td>Shift Supervisor</td>
<td>Training Coordinator</td>
</tr>
<tr>
<td>3</td>
<td>Training Coordinator</td>
<td>Training Coordinator</td>
</tr>
<tr>
<td>Shift Supervisor</td>
<td>Monitoring Center Manager</td>
<td>Monitoring Center Manager</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Minimum Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trainee</td>
<td>85%</td>
</tr>
<tr>
<td>1</td>
<td>85%</td>
</tr>
<tr>
<td>2</td>
<td>85%</td>
</tr>
<tr>
<td>3 / Shift Supervisor</td>
<td>90%</td>
</tr>
</tbody>
</table>

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.
## 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

| 3.2 | Monitoring Center Staff | a. Enrolling participants via the Internet for immediate activation of all monitoring services; |
| 3.3 | Monitoring Center Staff | b. Activating/installing both monitoring and tracking equipment on participants; |

**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 enrolling participants via the Internet for immediate activation of all monitoring services.
### 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;**

**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, 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.
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.

### SECTION D  Monitoring Services

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Monitoring Services</td>
<td>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.</td>
<td>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...</td>
</tr>
</tbody>
</table>
monitoring center.

IMPORTANT SENTINEL ADVANTAGE: 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.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>Monitoring Services&lt;br&gt;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>
</tr>
<tr>
<td></td>
<td>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 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 RF and Alcohol thereby creating multiple different contact points, potentially doubling and/or tripling workloads for officers/users.)</td>
</tr>
<tr>
<td>4.3</td>
<td>Monitoring Services&lt;br&gt;The Vendor’s Monitoring Center service must be able to tailor the level of alert notification to meet individual Agency needs or protocols.</td>
</tr>
</tbody>
</table>
|         | 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 safety 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
| 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. |
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.

---

*Access Control Choices*

<table>
<thead>
<tr>
<th>Manage Password (Change)</th>
<th>Change User Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Peer Email</td>
<td>Allows a user to enter an enrollment for another user that is in the same organization.</td>
</tr>
<tr>
<td>Peer View</td>
<td>Allows a user to view other users’ information that are in the same organization.</td>
</tr>
<tr>
<td>Subordinate View</td>
<td>Allows a user to view users that are found in organizations underneath their organization.</td>
</tr>
<tr>
<td>Subordinate Edit</td>
<td>Allows a user to edit users that are found in organizations underneath their organization.</td>
</tr>
<tr>
<td>Peer Edit</td>
<td>Allows a user to edit other users’ information that are in the same organization.</td>
</tr>
<tr>
<td>Web Patrol Admin</td>
<td>Allows a user to view tabs that are only visible to administrators.</td>
</tr>
</tbody>
</table>
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.

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
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.

<table>
<thead>
<tr>
<th>4.7</th>
<th>Monitoring Services</th>
<th>b. Data/Curfew changes;</th>
</tr>
</thead>
</table>

**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.
| 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; | **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. **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. |
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.
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.
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 on US
- EM Program Totals
- Equipment Last Call Date
- Inventory Returns
- Inventory Shipped to Agency
- Low Battery Status
<table>
<thead>
<tr>
<th>No Leaves or Enters</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Schedule Entered</td>
</tr>
<tr>
<td>Notification History by Officer</td>
</tr>
<tr>
<td>Officer Caseload</td>
</tr>
<tr>
<td>Officer User Report</td>
</tr>
<tr>
<td>Open Returns</td>
</tr>
<tr>
<td>Organization Key Alerts</td>
</tr>
<tr>
<td>Overdues</td>
</tr>
<tr>
<td>Participant Not Home</td>
</tr>
<tr>
<td>Participant Event History</td>
</tr>
<tr>
<td>Participant Location Report</td>
</tr>
<tr>
<td>Participant Notification History</td>
</tr>
<tr>
<td>Participants Currently in Violation</td>
</tr>
<tr>
<td>Schedule Out After Hours</td>
</tr>
<tr>
<td>Tech Issues</td>
</tr>
<tr>
<td>Termination Outcomes</td>
</tr>
<tr>
<td>Violations Summary by Participant</td>
</tr>
<tr>
<td>Web Only</td>
</tr>
<tr>
<td>Enrolled Participant Roster greater than 60 days</td>
</tr>
</tbody>
</table>

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

c. 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.
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 safety of its participants. For example, an agency may choose to outline three (3) notification profiles:
### 4.13 Monitoring Services

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

- **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.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Requirement</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.14</td>
<td>Monitoring Services</td>
<td>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.</td>
<td><strong>Sentinel exceeds this requirement.</strong> 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:</td>
</tr>
</tbody>
</table>
|         |             |             | ▪ 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.

<table>
<thead>
<tr>
<th>4.16 Monitoring Services</th>
<th>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.</th>
</tr>
</thead>
</table>

**Sentinel meets this requirement.** Sentinel provides agencies with toll free phone and fax contact numbers, accessible 24 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**
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

Table: Alert Notifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Alert Notifications</td>
<td>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:</td>
<td>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.</td>
</tr>
<tr>
<td>5.2</td>
<td>Alert Notifications</td>
<td>a. Non-compliance with pre-determined curfews;</td>
<td>Sentinel meets this requirement. Sentinel provides alert notifications for a wide array of non-compliance events with pre-determined curfews including:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave During Curfew</td>
<td>The participant’s PTX2 has left the range of the PHMU during curfew.</td>
</tr>
<tr>
<td>Return During Curfew</td>
<td>The participant’s PTX2 has come into range of the PHMU during curfew.</td>
</tr>
<tr>
<td>Curfew Start Present</td>
<td>The participant’s Curfew has started and their PTX2 is present.</td>
</tr>
<tr>
<td>Curfew Start Not Present</td>
<td>The participant’s Curfew has started and their PTX2 is not present.</td>
</tr>
<tr>
<td>Curfew Start Status Unknown</td>
<td>The participant’s Curfew has started, but their PTX2 presence is unknown due to HMU Overdue</td>
</tr>
<tr>
<td>Curfew Start Status Update-Present</td>
<td>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.</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Curfew Start Status Update-Not Present</td>
<td>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.</td>
</tr>
<tr>
<td>Curfew Start Status Update-Review Events</td>
<td>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.</td>
</tr>
<tr>
<td>Curfew End Present</td>
<td>The participant's Curfew has ended and their PTX2 is present.</td>
</tr>
<tr>
<td>Curfew End Not Present</td>
<td>The participant's Curfew has ended and their PTX2 is not present.</td>
</tr>
<tr>
<td>Curfew End Status Unknown</td>
<td>The participant's Curfew has ended, but their PTX2 presence is unknown due to HMU Overdue.</td>
</tr>
<tr>
<td>Curfew End Status Update-Present</td>
<td>Enter late that occurred prior to the Curfew End, resulting in a ‘Curfew End Status Update-Present’ event.</td>
</tr>
<tr>
<td>Curfew End Status Update-Not Present</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter</td>
<td>The participant’s PTX2 has come into range of the PHMU.</td>
</tr>
<tr>
<td>Leave</td>
<td>The participant’s PTX2 has left the range of the PHMU.</td>
</tr>
<tr>
<td>Short Leave</td>
<td>The participant's PTX2 left the range of the PHMU for less than the leave window.</td>
</tr>
<tr>
<td>Enter During Mandatory Schedule</td>
<td>The participant’s PTX2 has come into range of the PHMU during their Mandatory leave time.</td>
</tr>
<tr>
<td>Leave During Mandatory Schedule</td>
<td>The participant's PTX2 has left the range of the PHMU after they were required to be out.</td>
</tr>
<tr>
<td>Mandatory Schedule Start Present</td>
<td>The participant's Mandatory leave time has started and their PTX2 is present.</td>
</tr>
<tr>
<td>Mandatory Schedule Start Not Present</td>
<td>The participant's Mandatory leave time has started and their PTX2 is not present.</td>
</tr>
<tr>
<td>Mandatory Schedule Start Status Update-Present</td>
<td>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.</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mandatory Schedule Start Status Update-Present</td>
<td>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.</td>
</tr>
<tr>
<td>Mandatory Schedule Start Status Update-Not Present</td>
<td>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.</td>
</tr>
<tr>
<td>Mandatory Schedule Start Status Update-Review Events</td>
<td>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.</td>
</tr>
<tr>
<td>Mandatory Schedule End Present</td>
<td>The participant's Mandatory leave time has ended and their PTX2 is present.</td>
</tr>
<tr>
<td>Mandatory Schedule End Not Present</td>
<td>The participant's Mandatory leave time has ended and their PTX2 is not present.</td>
</tr>
<tr>
<td>Mandatory Schedule End Status Update-Present</td>
<td>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.</td>
</tr>
</tbody>
</table>
5.4 Alert Notifications

<table>
<thead>
<tr>
<th>c. Tampering with the transmitter or any of its components;</th>
</tr>
</thead>
</table>

**Sentinel exceeds this requirement.** Sentinel provides alert notifications for a wide array of transmitter tamper events including:

<table>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</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.
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 vendors 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.
### 5.5 Alert Notifications

<table>
<thead>
<tr>
<th><strong>Sentinel meets this requirement.</strong> Sentinel provides alert notifications for a wide array of receiver tamper events including:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification Exceptions</strong></td>
</tr>
<tr>
<td>HMU Tamper</td>
</tr>
<tr>
<td>HMU Tilt</td>
</tr>
<tr>
<td>PHMU Forced Power Down</td>
</tr>
<tr>
<td>Power Disconnect</td>
</tr>
<tr>
<td>Communication No Dial Tone</td>
</tr>
<tr>
<td>Telephone Disconnect</td>
</tr>
</tbody>
</table>

### 5.6 Alert Notifications

<table>
<thead>
<tr>
<th><strong>Sentinel exceeds this requirement.</strong> 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:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification Exceptions</strong></td>
</tr>
<tr>
<td>HMU Overdue</td>
</tr>
<tr>
<td>Scheduled Report</td>
</tr>
<tr>
<td>PHMU Report Schedule Changed (Old, New)</td>
</tr>
<tr>
<td>Immediate Call In Request</td>
</tr>
</tbody>
</table>
### 5.7 Alert Notifications

<table>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

---

### 5.8 Alert Notifications

<table>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

---

**Sentinel exceeds this requirement.** Sentinel provides alert notifications for a wide array of loss and/or restoration of telecommunications events including:

**Sentinel meets this requirement.** Sentinel provides alert notifications for a wide array of loss and/or restoration of alternating current (AC) power events including:
### 5.9 Alert Notifications

**h. Detection of low power or battery malfunctions in the transmitter or Receiver;**

**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>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### 5.10 Alert Notifications

**i. Movement of the Receiver to an unauthorized telephone line;**

**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>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</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.

### 5.11 Alert Notifications

**j. Detection of operating malfunctions in the Receiver or transmitter.**

**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>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Notification Exceptions</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HMU Diagnostics</td>
<td>The PHMU has provided internal operating and diagnostic information.</td>
</tr>
<tr>
<td>HMU System Source</td>
<td>The PHMU has provided internal operating and diagnostic information.</td>
</tr>
<tr>
<td>Out of Sync.</td>
<td>The PTX2 and PHMU may be out of sync. Repeat occurrences may require further investigation.</td>
</tr>
<tr>
<td>Remote PTX2 Change</td>
<td>The PTX2 being monitored has been changed remotely.</td>
</tr>
<tr>
<td>Remote PTX2 Remove</td>
<td>A PTX2 has been removed from the PHMU remotely.</td>
</tr>
<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>
</tbody>
</table>
| 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 safety 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. |
## SECTION F Reports

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Reports</td>
<td>Please provide a list of typical detailed reports the Vendor provides to current or previous customers.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Active Inactive Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Active Participant Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Additions Deletions Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Agency Inactive Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Alarm Step History</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Alarm Step History by Participant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Alerts Not Viewed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Caseload by Participant</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Caseload Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Caseloads Not Viewed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Caseloads Viewed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Curfew Schedules</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Current Open Alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Daily Status Exception</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Daily Status Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Daily Status Exception Report by Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Daily Status Exception Report by Region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Daily Status Exception Only Report by Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domestic Billing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domestic Billing by Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Drive-By</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Electronic Monitoring Participants en US</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• EM Program Totals</td>
</tr>
</tbody>
</table>
| 6.2 Reports | **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). |

- 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
### 6.3 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.
## Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

<table>
<thead>
<tr>
<th>Section</th>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7</td>
<td>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;</td>
<td><strong>Sentinel meets this requirement.</strong> 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.</td>
</tr>
<tr>
<td>6.8</td>
<td>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;</td>
<td><strong>Sentinel meets this requirement.</strong> 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: <strong>Drive Bys:</strong> Listing of Drive bys by serial number and location.</td>
</tr>
<tr>
<td>6.9</td>
<td>g. Daily active Participant Roster Report.</td>
<td><strong>Sentinel meets this requirement.</strong> 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: <strong>EM Participants:</strong> List of participants on electronic monitoring. Additionally, the SenTrak Caseload Management screen provides this data via the web-based system.</td>
</tr>
<tr>
<td>6.10</td>
<td>On-demand reports with user defined fields as requested by Agency.</td>
<td><strong>Sentinel meets this requirement.</strong> 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</td>
</tr>
</tbody>
</table>
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.

### SECTION G. Account Management and Training

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Account Management</td>
<td>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.</td>
<td>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 expeditiously, 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.</td>
</tr>
</tbody>
</table>
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 ADVANTAGE: 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
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

<table>
<thead>
<tr>
<th>7.2</th>
<th>Account Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.2</th>
<th>Account Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
<td></td>
</tr>
</tbody>
</table>

- 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.
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 expeditiously, 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.
<table>
<thead>
<tr>
<th>7.4</th>
<th>Training</th>
</tr>
</thead>
</table>

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 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 ADVANTAGE:** 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 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.

<table>
<thead>
<tr>
<th>7.5</th>
<th>Training</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6</td>
<td>Training</td>
<td>Deleted</td>
</tr>
</tbody>
</table>
**Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders**

| 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. |

---

### SECTION H  General Equipment, Transmitter and Receiver Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Description</th>
<th>Describe how Vendor passes, meets or exceed</th>
</tr>
</thead>
</table>

---

Page 138 of 541
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:  

---  

8.2 Equipment | The equipment manufacturer shall have an ISO 9001 certification.  

---  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentinel meets this requirement.</td>
<td></td>
</tr>
</tbody>
</table>
| **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 |

---  

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. |
| 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. |
| 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 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.

**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.

**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:
<table>
<thead>
<tr>
<th>Transmitter Features</th>
<th>RF Patrol® PTX2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant Worn Device</td>
<td>Unique watch-size transmitter device for wrist or ankle</td>
</tr>
<tr>
<td>Device Specifications</td>
<td>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</td>
</tr>
<tr>
<td>Tamper Alert</td>
<td>Yes, patented multiple fiber-optic circuits</td>
</tr>
<tr>
<td>Transmitter Battery Life</td>
<td>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</td>
</tr>
<tr>
<td>Activation</td>
<td>On-site programmable range during installation (no software required)</td>
</tr>
<tr>
<td>Deactivation</td>
<td>Shutdown of transmitter via two-way RF link</td>
</tr>
<tr>
<td>Required Assembly of Transmitter</td>
<td>Easiest to install in the industry Transmitter is a sealed unit Four (4) easy to install transmitter pieces</td>
</tr>
<tr>
<td>Transmission Signal</td>
<td>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</td>
</tr>
</tbody>
</table>

**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.
Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

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

<table>
<thead>
<tr>
<th>PHMU Features</th>
<th>RF Patrol® Landline</th>
<th>RF Patrol® Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>Fully integrated one (1) piece unit Dual antennas and transceivers</td>
<td>Fully integrated one (1) piece unit Dual antennas and transceivers</td>
</tr>
<tr>
<td><strong>PHMU Specifications</strong></td>
<td>Smallest and lightest available on the market at 7.5 X 8.6 X 1.7 inches and weighs 16 ounces 100% humidity resistant</td>
<td>Smallest and lightest available on the market at 7.5 X 8.6 X 1.7 inches and weighs 16 ounces 100% humidity resistant</td>
</tr>
<tr>
<td><strong>Tamper Alert</strong></td>
<td>Yes, including tilt detection</td>
<td>Yes, including tilt detection</td>
</tr>
<tr>
<td><strong>Back-up Battery Life</strong></td>
<td>48 hours of continuous operation</td>
<td>48 hours of continuous operation</td>
</tr>
<tr>
<td><strong>Front Panel LED Display Activation</strong></td>
<td>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</td>
<td>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</td>
</tr>
<tr>
<td><strong>Deactivation</strong></td>
<td>Shutdown of transmitter (PTX2) via two-way RF link</td>
<td>Shutdown of transmitter (PTX2) via two-way RF link</td>
</tr>
<tr>
<td><strong>Required Assembly</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Transmission Signal</strong></td>
<td>Transceiver technology with the PTX2 Landline communication with the monitoring center</td>
<td>Transceiver technology with the PTX2 Wireless cellular communication with the monitoring center</td>
</tr>
<tr>
<td>8.6 Equipment</td>
<td>Transmitters and Receivers shall be field replaceable and interchangeable without the need to return them to the Vendor.</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Sentinel meets this requirement.</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.7 Equipment</th>
<th>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.</th>
</tr>
</thead>
</table>
|               | **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. |

<table>
<thead>
<tr>
<th>Multiple Transmitters</th>
<th>Ability to monitor up to 50 PTX2s at the same time</th>
<th>Ability to monitor up to 50 PTX2s at the same time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Detection</td>
<td>Detects and reports unauthorized PTX2 units in range</td>
<td>Detects and reports unauthorized PTX2 units in range</td>
</tr>
<tr>
<td>Memory/Storge</td>
<td>Internal non-volatile memory capable of storing 90 days of events indefinitely</td>
<td>Internal non-volatile memory capable of storing 90 days of events indefinitely</td>
</tr>
</tbody>
</table>
### Contract 00212 with Sentinel Offender Services for Electronic Monitoring of Offenders

<table>
<thead>
<tr>
<th>Step 1: Prepare the PTX2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert end of the Band that has clip pre-attached into one end of the PTX2 housing</td>
<td></td>
</tr>
<tr>
<td>Listen for two clicks to ensure the band is properly engaged</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2: Sizing the PTX2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrap the PTX2 around the participants ankle until snug</td>
<td></td>
</tr>
<tr>
<td>Measure to the closest hole to the edge of the face of the PTX2</td>
<td></td>
</tr>
<tr>
<td>Once the appropriate fit is established, remove the PTX2 from the participant and use the Guillotine Cutting Tool to cut the Band</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3: Attaching the PTX2 to the Ankle</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide the Clip over the trimmed end of the Band until the holes on the Clip are aligned with the holes on the Band</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Wrap PTX2 Band around ankle of participant</td>
<td></td>
</tr>
<tr>
<td>Insert this end of the Band into one end of the PTX2 housing</td>
<td></td>
</tr>
<tr>
<td>Listen for two clicks to ensure the band is properly engaged</td>
<td></td>
</tr>
</tbody>
</table>

In the interest of public safety, Sentinel believes that it is 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.
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’s 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)
<table>
<thead>
<tr>
<th>Section</th>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.9</td>
<td>Equipment</td>
<td>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. <strong>Sentinel meets this requirement.</strong> 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.</td>
</tr>
<tr>
<td>8.10</td>
<td>Transmitter</td>
<td>Device must not pose a safety hazard or unduly restrict the activities of the participant. Must be light weight, small and water-resistant. <strong>Sentinel exceeds this requirement.</strong> 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.</td>
</tr>
<tr>
<td>8.11</td>
<td>Transmitter</td>
<td>The transmitter shall be encased in a water-resistant case that is corrosion resistant and impervious to chemical solvents and detergents. <strong>Sentinel meets this requirement.</strong> 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.</td>
</tr>
</tbody>
</table>
| 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:

- **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. |

| 8.12 (Continued) | | |

| 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:YEVM06BPHMUL08 |

| 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 | 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 participant's 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 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.
8.16 Transmitter
Neither the transmitter, receiver, straps, fasteners nor clips, etc. used to install the transmitter shall be available to the general public.

**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.

8.17 Transmitter
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.

**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>
<thead>
<tr>
<th>Notification Exceptions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMTR Low Battery</td>
<td>The PTX2 battery is low and requires return to Sentinel.</td>
</tr>
</tbody>
</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** 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.
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 atrribution 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.
| 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® 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® 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.

<table>
<thead>
<tr>
<th>8.20</th>
<th>Transmitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**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