SENTINEL®

RESPONSE TO RFP N°. 2-2018

Electronic Monitoring for Community Corrections

LEXINGTON-FAYETTE URBAN COUNTY GOVERNMENT
TODD SLATIN – PURCHASING DIRECTOR
200 EAST MAIN STREET
ROOM 338 | GOVERNMENT CENTER
LEXINGTON, KY 40507

PRESENTED BY

D.J. WILLIAMSON| REGIONAL SALES EXECUTIVE
SENTINEL OFFENDER SERVICES, LLC
201 TECHNOLOGY DRIVE | IRVINE, CA 92618
P| 765.247.9101 F| 800 327 1178
E| DWILLIAMSON@SENTINELADVANTAGE.COM

DUE FEBRUARY 8, 2018 AT 2:00 P.M.

SENTINEL®

1 TRANSMITTAL LETTER

February 6, 2018

Todd Slatin – Purchasing Director
Lexington-Fayette Urban County Government
200 East Main Street
Room 338, Government Center
Lexington, KY 40507

Re: Sentinel Offender Services Proposal Response Submission to RFP No. 2-2018

Dear Mr. Slatin:

Sentinel Offender Services, LLC ("Sentinel"), is pleased to provide this response to the Lexington-Fayette Urban County Government (LFUCG) request for proposal for the provision of Electronic Monitoring for the Division of Community Corrections (Division) as the best and most proven solution to address the requirements and needs of the program. Sentinel management has carefully reviewed the RFP Scope of Services, terms, conditions, requirements, and addendums, including the answers to questions, and we have a clear and concise understanding of the LFUCG's request for Electronic Monitoring for Community Corrections proposals.

Sentinel is a well-qualified provider and fully prepared to successfully collaborate with the Division by developing and implementing an effective state-of-the-art electronic monitoring program that is uniquely tailored to the distinct individual programmatic needs of the agency. As one of the nation's leading providers of electronic monitoring products and services, Sentinel will act as the prime provider for all of the equipment and services offered and delivered for the Electronic Monitoring for Community Corrections program. As a result of being the prime provider, without relying on any subcontractor for execution and delivery of critical monitoring service elements of its proposed offering, Sentinel believes our products, services, and support offers the best and most proven solution to address the individual requirements and needs of the Division.

Our industry leading experience, expertise and proven ability positions Sentinel to be the optimum choice for this contract. The LFUCG can award a contract for Electronic Monitoring for Community Corrections to Sentinel with full confidence that the current program will have access to industry leading, state-of-the-art equipment and services, while being managed and operated successfully by a team of professionals with the most experience in the industry.

201 TECHNOLOGY DRIVE | IRVINE, CALIFORNIA 92618
P| 800 589 6003 F| 800 327 1178 W| SENTINELADVANTAGE.COM

SENTINEL®

As one of the nation's leading providers of electronic monitoring and offender supervision programs, Sentinel welcomes the opportunity to collaborate with Division for the provision of programmatic services for the agency. As a company, Sentinel offers the following advantages:

Corporate Stability

Sentinel has been providing offender supervision equipment and services to criminal justice agencies for 25 years, maintaining the same ownership since inception, which is an achievement no other bidding vendor can claim. Since beginning operations in 1993, Sentinel has been entirely focused on providing criminal justice agencies with the utmost in service and equipment, along with the personnel to assist agency staff with the operation of programs.

Summary of Offering

We understand the objectives of the program and are specifically proposing the use of state-of-the-art radio frequency monitoring, global positioning satellite tracking, remote breath alcohol testing, and secure web-based monitoring and data hosting services to provide a comprehensive electronic monitoring program for participants through the utilization of innovative technologies and services to address the requirements of the program. Sentinel has proposed a complete turnkey electronic monitoring solution with the use of our proven latest generation RF Patrol™ radio frequency electronic monitoring solution, OM400™ one-piece global positioning satellite tracking solution and BA/RT™ handheld breath alcohol testing in real-time with the support of our Internet-based monitoring systems, 24-hour-a-day monitoring center support, and experienced corporate quality assurance program managed through our California headquarters.

In addition to these field-proven technologies, we are highly experienced in delivering voice verification services, full-service case management and collections, and day reporting services. No other company in the industry has the ability to offer the wide-range of equipment and service choices we have to offer the Division.

Qualified Staff

Sentinel will supply trained and experienced staff during the term of this new contract. Sentinel has trained staff in place who will ensure that the program is operating efficiently and in accordance with the LFUCG's expectations. Sentinel has a team of staff members currently assembled who will add significant value because of their direct experience and extensive knowledge of the electronic monitoring industry and stand ready to transition the Division's current program in a seamless and smooth manner. Sentinel's dedicated Project Team consisting of Ms. D.J. Williamson, Regional Sales Executive, who brings 25 years in the electronic monitoring industry, while Mr. Darin Simion, Regional Account Manager, has 14 years of professional experience in the electronic monitoring / community

201 TECHNOLOGY DRIVE | IRVINE, CALIFORNIA 92618
P| 800 589 6003 F| 800 327 1178 W| SENTINELADVANTAGE.COM

corrections industry. Sentinel is proud to have a dedicated Project Team of this magnitude that has nearly 40 years of combined industry experience. Under the guidance provided by this team, and in close coordination with the LFUCG, Sentinel will operate the Electronic Monitoring for Community Corrections program outlined in this Request for Proposal.

Technical Expertise

Sentinel's core business operations include electronic monitoring programs. Sentinel provides uninterrupted 24 hour a day, seven (7) day a week, 365 days a year electronic monitoring and supervision services to nearly 250 agencies across the United States. Sentinel's professional staff of over 200 employees is solely dedicated to providing services within the offender management market delivering monitoring to tens-of-thousands of individual participants on a daily basis through its monitoring centers and a nationwide network of field offices. Sentinel has extensive experience with every aspect of community supervision.

Our team provides a full-continuum of supervision solutions, ranging from low-risk participants to the highest risk participants in the industry. Sentinel's Best in Class approach to problem solving and our ability to listen, understand and execute on our customer's needs with the right equipment, services, team members, internally designed proprietary software and any combination of field services required, has made us one of the top electronic monitoring providers in the industry for over 20 years. The ability to offer this full-continuum of services to the Division is evidence of Sentinel's ability to provide extensive supervision scalability and program adaptability for the program using electronic monitoring equipment and services.

Quality of Service

Sentinel is dedicated to delivering quality services, equipment and software and has achieved ISO Certification for the Design, Production, Installation, and Servicing of Electronic Monitoring Products. ISO Certification is important to our customers, as it shows that Sentinel is committed to quality and ensures that we have audited systems, processes, and procedures in place that cover all aspects of our business.

Closing Statements

It is Sentinel's belief that this combination of extensive experience in the criminal justice industry, unique technology and service offerings along with our exceptional customer service and support capabilities provides the "Best Value" solution for the LFUCG's Electronic Monitoring program for Community Corrections.

As Regional Sales Executive, I am authorized to negotiate this proposal, answer questions, and provide clarification on behalf of Sentinel and will act as Contract Manager for any resulting contract. Dennis Fuller, Chief Financial Officer, is authorized to bind the company to contract. Please feel free to contact me directly at 765.247.9101, via email at dwilliamson@sentineladvantage.com, by fax at

800.327.1178, or U.S. mail at 201 Technology Drive, Irvine, CA 92618. Again, thank you for this opportunity to provide GPS tracking and alcohol testing equipment and services to the Lexington-Fayette Urban County Government and the Division of Community Corrections.

Sincerely,

D.J. Williamson
Regional Sales Executive

Dennis Fuller
Chief Financial Officer

SENTINEL®

201 TECHNOLOGY DRIVE | IRVINE, CALIFORNIA 92618
P| 800 589 6003 F| 800 327 1178 W| SENTINELADVANTAGE.COM

2 TABLE OF CONTENTS

3 EXECUTIVE SUMMARY

Sentinel's core business operations are centered on providing state-of-the-art equipment and world class services to electronic monitoring programs. We provide 24 hour a day, seven (7) day a week, 365 day a year electronic monitoring and supervision services to nearly 250 agencies across the United States from our ISO 9001:2008 Certified National Monitoring Center. Our professional staff of over 200 employees is solely dedicated to providing services within the offender management market. We provide monitoring to tens-of-thousands of individual participants on a daily basis through our monitoring center and a nationwide network of field offices.

We have extensive experience with every aspect of community supervision including a full-continuum of supervision solutions ranging from solutions that support low-risk participants who are monitored through voice verification or traditional radio frequency monitoring, as well as higher risk participants who are monitored through global positioning satellite tracking. We also provide solutions such as a kiosk that is used for check-in reporting and state-of-the-art alcohol monitoring including both in-home and portable breath testing as well as transdermal alcohol monitoring. The ability to offer this full continuum of services is evidence of Sentinel's ability to provide extensive supervision scalability and program adaptability for our customers as they grow and require a wider breath of monitoring solutions. Additionally, all of our monitoring services are performed through Sentinel's National Monitoring Center located in Irvine, California.

Since our beginning back in 1993, Sentinel's sole focus remains to this day on providing electronic monitoring services to criminal justice agencies and organizations, and since our inception, we have had more than 1,500,000 participants successfully complete their programs through our community-based monitoring services. *All of Sentinel's services, products and technologies are specifically designed for corrections supervision and meet or exceed the requirements of the agencies we serve.*

In our 25 years of service, we have provided a wide array of services to offender supervision programs nationwide. We monitor participants that are pre-trial, post-sentence, and in custody for those agencies we service, *including both adult and juvenile populations*. We continue to exhibit extraordinary depth in qualifications and experience, and we administer all aspects of our solutions-based programs in partnership, and in complete compliance, with agency-specific directions.

We provide corrections agencies, sheriff's departments, probation departments, and courts nationwide with more electronic monitoring and offender solutions than any other service provider. We offer a broad menu of supervision solutions, including:

+ Global Positioning Satellite (GPS) Tracking
+ Radio Frequency (RF) Monitoring
+ Drug and Alcohol Testing Services
+ Voice Verification Programs
+ Offender-Funded Programs
+ Kiosks for Check-in and Collections Programs

- Court Programs
- Fines, Fees, and Restitution Collection Programs
- Case Management Services
- Sentinel Success Center Programs

—IMPORTANT SENTINEL ADVANTAGE—

As a company, Sentinel specifically:

- Offers 25 years of continuous electronic monitoring experience including RF monitoring, voice verification, GPS tracking, and alcohol monitoring;
- Offers proprietary monitoring software and case management software that is 100% web-based and provides authorized agency staff the ability to access real-time data on their case load;
- Currently monitors tens-of-thousands of active participants daily;
- Meets or exceeds all of the programmatic needs for monitoring and technical support;
- Offers the unparalleled ability to serve agency-specialized needs with industry-leading and innovative program models;
- Employs the most qualified and educated staff in the industry, with comprehensive knowledge specific to the electronic monitoring programs;
- Possesses all permits, licenses and professional credentials necessary to supply products and perform services as specified under this solicitation; and
- Operates our own 24 hour 7 day a week ISO 9001-2008 certified monitoring center without the use of subcontractors.

3.1 Experience

With over two (2) decades in operation, Sentinel is one of the leading companies in the offender supervision arena. We have operations in 30+ states, and work with some of the largest programs in the country including, Los Angeles County, Miami-Dade County and the states of Mississippi, Kansas, Nevada, and Connecticut. We are highly experienced with diverse program populations and currently employ educated and trained staff to provide services to multi-lingual and disabled persons.

Sentinel has shown to each of our customers that we execute upon our commitment to providing services that meet or exceed their equipment and distinct service needs. Over the last 20-plus years we have gained knowledge and experience in how to design programs that are based on clear communication, strict compliance to program requirements, and a focus on providing world class services to our customers. We are committed to ensuring that the programs operated on behalf of federal, state, and local agencies support their goal of protecting public safety by providing quality service and innovative solutions. LFUCG can be assured that Sentinel will provide unsurpassed experience, equipment, and the same commitment and dedication to the Electronic Monitoring for Community Corrections program.

We recognize the importance of each participant understanding the program rules and expectations to ensure the best outcome for both the participant and the program in order to increase public safety and reduce the costs of incarceration for low- to medium-risk offenders and potential repeat offenders. We continue to exhibit extraordinary depth in qualifications and experience and will draw on our experience to continue to provide a world-class program to successfully achieve the LFUCG's goals and objectives of promoting public safety, the prevention and reduction of criminal activity through best practices, and improved community supervision practices and procedures.

Sentinel strives to develop and maintain strong relationships with our customers based upon integrity, openness, and accountability. As an example, we have provided six (6) references, which are fully operational programs using similar solutions to those presented in this proposal and of similar size to the Electronic Monitoring for Community Corrections program, within proposal section **4. Scope of Work / Q. References** (page 130).

3.2 Project Team

We have assembled a multi-faceted Project Team to provide the program with all services including but not limited to account management, remote technical assistance, customer support, inventory, billing, and information technology support. The Project Team assembled for this program includes several staff members that add significant value. Ms. D.J. Williamson, Regional Sales Executive, has over 25 years of experience within the criminal justice and electronic monitoring industries. Mr. Darin Simion, Regional Account Manager, has over 14 years of experience within the electronic monitoring industry. Ms. Williamson and Mr. Simion will be tasked with assessing the program against the industry best-practices to propose creative solutions to the agency to enhance effectiveness. Ms. Williamson will provide corporate oversight for the contractual cycle of the program while Mr. Simion will provide regional account management support during the program lifecycle.

The comprehensive monitoring of the program's client populations is comprised of a combined effort between the agency, our proposed Project Team, and our National Monitoring Center. We do not subcontract any of our monitoring services that we are offering as part of this proposal. The following are descriptions of the associated project tasks of operational staff responsible for the program.

D.J. WILLIAMSON | Regional Sales Executive
Ms. D.J. Williamson brings 25 years of electronic monitoring and criminal justice experience to the Sentinel team. During her fifteen (15) years with Sentinel, Ms. Williamson has held multiple positions within the company and is currently one of our Regional Sales Executives. Her experience includes overseeing day-to-day program development and operations, managing multiple regional offices, and providing presentations and demonstrations to top level executives, Legislators, Judges and Chiefs. She will provide support throughout the RFP process for Sentinel's corporate office during the sales cycle. Ms. Williamson will also provide corporate oversight for the contractual cycle as well as back-up technical support to the agency and purchasing department. Ms. Williamson completed her BS degree in Criminal Justice with a minor in Business Administration from Indiana State University in Terre Haute, Indiana. Her responsibilities will include:

- Support and liaison status throughout the quote phase and contract negotiation phase between the agency and Sentinel's corporate office;
- Corporate oversight for the contractual cycle as well as back-up technical support to the agency's programs and purchasing department; and
- Aiding in the post-award implementation and transition phases for this contract.

DARIN SIMION | Regional Account Manager

Darin Simion is responsible for the management of a customer portfolio which includes providing customer logistics, training, and consultancy. In 2004, Mr. Simion began working for Marion County Community Corrections (Indiana) as a field deputy patrolling the community and managing a caseload of 300 home detention and pretrial offenders. He has been involved in the set-up and supervision of the agency-run monitoring centers for the Marion County and North Carolina electronic monitoring programs and possesses extensive experience with developing and delivering training programs. Mr. Simion joined G4S/Sentinel in 2007, and has held several industry related positions such as Community Corrections Officer, Trainer, and Electronic Monitoring Specialist. For this program, Mr. Simion will:

- Conduct/assist with trainings and implementation of the program; and
- Be responsible for daily, weekly, and monthly reviews of inventory reports and any required KPI Reports as per the contract.

MELISSA STARR | Vice President of Field Operations

Ms. Starr provides and/or is responsible for the management oversight to our Regional Account Managers as well as Sentinel's on-site and branch office personnel; conducting / assisting with training and the implementation of any new equipment offerings, and attending meetings as requested by the supervising agency. Ms. Starr began her career in the electronic monitoring industry nearly 17 years ago with Sentinel Offender Services managing an active offender caseload of 150 participants. She was quickly promoted through the Company to Branch Manager, Project Director and then Field Operations Manager of Western Region where she was responsible for all branch operations and business development.

In 2010, Ms. Starr accepted an opportunity to become Vice President of Customer Service with an industry competitor. For four (4) years she gained valuable senior leadership experience and managed staff and accounts on a national basis. As we entered 2014, Ms. Starr and Sentinel were both pleased to have her back as the Vice President of Field Operations. Ms. Starr has developed relationships with agencies across the country and has helped them design, implement and manage successful alternative to incarceration programs using innovative hardware and software solutions. She focuses on program integrity, consultation and customer service. As a true industry veteran, her expertise in relationship building with customers and team building with staff has resulted in a contract retention rate of over 95 percent in a very volatile and competitive industry. She will be responsible for:

- All field staff, guiding branch offices in contract retention, and;
- Ensuring adherence with strict SOP's; and business development.

JEFF MCDANIEL | National Service Center Director

Mr. McDaniel manages the National Monitoring Center located in Irvine, CA. He is responsible for the performance management of the staff along with ensuring the customer experience is cared for at every touch point. Mr. McDaniel joined the Sentinel Leadership team in 2016 and brings with him over 15 years managing contact centers in the telecom industry. While working with the telecom industry he managed domestic internal contact centers and focused on strategic partner relationships domestically and internationally. He focuses on delivering exceptional customer service while managing effective operations throughout the Monitoring Center. His expertise in team building with staff while delivering on operational efficiencies has resulted in successful contact center management throughout his career. Mr. McDaniel will be responsible for the Monitoring Center operations for this program. His responsibilities will include:

+ Supervising operations for the monitoring center;
+ Supervising the provision of services provided by the customer support center;
+ Ensuring that contracted services are provided as outlined in contract requirements; and
+ Developing policies and strategic plans for monitoring center operations, including new program introduction and notification policies, training and quality assurance standards.

CONTINUOUS MONITORING CENTER OPERATIONS AND SUPPORT

Sentinel's National Monitoring Center is the focal point of our state-of-the-art facility, located in Irvine, California. This is the central location from which all monitoring center activities are conducted and information is disseminated. The monitoring center is a separate, self-supporting node within the facility which is approximately 3,000 square feet and handles over 50,000 calls on a daily basis. All monitoring services will be provided by Sentinel personnel and equipment. *Sentinel's direct provision of monitoring duties eliminates concerns found with other vendors who have no direct control over their subcontractor's monitoring center.*

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own *monitoring center that is operational 24* hours *a day, seven (7) days a week, 365 days a year.*

Sentinel strives to consistently recruit, employ and retain the best people and provide equal opportunity at all levels. Sentinel also provides expert field personnel whose experience includes contract management on federal, state and local levels. Current Sentinel account managers provide an extensive criminal justice and corrections background that enhances communication between the program managers and the field technical staff. Sentinel requires each employee to read and sign a Non-Disclosure Agreement, addressing the privacy and security of the agency and participant monitoring information. Sentinel also requires employment applicants to provide detailed background information, which is reviewed in the staffing evaluation process. To ensure the utmost maintenance of ethical standards and security for Sentinel's corrections customers, Sentinel requires all employees to pass criminal background checks as well as Sentinel's own rigorous screening requirements. Due to the sensitive nature of products and services, Sentinel does not employ individuals with felony records or misdemeanors of moral turpitude.

3.3 Minority-Owned (MBE) and Woman-Owned (WBE) Business Enterprises

Sentinel is committed to utilizing qualified minority/women-owned businesses to the greatest extent feasible in the procurement of goods, equipment and services. We recognize MBE/WBE's to be significant value-added and viable sources and look for opportunities to utilize MBE/WBE's whenever possible. Examples of our MBE / WBE contracts include Sentinel's largest printed circuit board (PCB) assembly houses, Trantronics, Inc., a minority-owned business enterprise located in California, and Sentinel's Employee Healthcare broker, Burnham Benefits, a woman-owned business enterprise located in California. Additionally, Sentinel actively seeks MBE and WBE companies to provide office supplies to our headquarters and branch office locations throughout the United States. Of Sentinel's $175,000.00 office supply budget for fiscal year 2017, four percent (4%) of Sentinel's office supply budget was spent with Minority-Owned Business while six percent (6%) of our budget was spent with Women-Owned Businesses.

Sentinel understands that Lexington-Fayette Urban County Government is requesting that 10% of this contract's annual budget is spent with MWDBE businesses, and we have reviewed the Lexington-Fayette County Government Certified MWDBE list located on the Web Site as well as the Commonwealth of Kentucky Certified MBE/WBE list; because the RFP is seeking public safety elements that consist of proprietary offender monitoring software, rental of electronic monitoring equipment, and the utilization of current county personnel, there are no opportunities to spend budget dollars with outside MWDBE vendors for the delivery of services as stated in the RFP.

Because of the nature of the services being provided, the importance of confidentiality to offender records and data, and the importance to security and public safety aspects involved with the monitoring center services being provided under the contract, often confidentiality clauses restrict the use of subcontractors. Also, Sentinel is the sole authorized provider of the system, monitoring software, 24/7 monitoring center services, including Sentinel Monitoring Center Operator's investigative calls being made directly to offenders placed in the program, and direct training and support to agency staff.

Sentinel will continue to make an exerted effort to spend budget dollars with other identified MWDBE vendors as the need emerges. Sentinel is familiar with submitting quarterly and/or annual reporting on MWDBE expenditures and agrees to submit the appropriate reports as requested in the RFP when contract dollars are spent with MWDBE vendors.

3.4 Offering to the Division

Sentinel is a well-qualified provider, fully prepared to successfully collaborate with the Lexington-Fayette Urban County Government (LFUCG) by developing and implementing effective, state-of-the-art electronic monitoring equipment and monitoring services that will provide services to offenders/defendants under community supervision within the County and the surrounding area. As one of the nation's leading providers of electronic monitoring products and services, Sentinel welcomes the opportunity to work in collaboration with the Division of Community Corrections for the provision of services for the Electronic Monitoring program. Sentinel is pleased to propose a program that offers the Division a complete turnkey electronic monitoring solution with the use of our RF Patrol™ radio frequency electronic monitoring solution, OM400™ one-piece GPS tracking solution, BA/RT™ portable

handheld breath alcohol testing device, and our Sentinel DNA™ monitoring system application with the support of our 24-hour a day monitoring center support staff and experienced corporate quality assurance program.

Our solution will provide the Division with: (1) access to a state-of-the-art Electronic Monitoring Program including all equipment, consumables, installation kits, and spares; 2) support services including a Regional Account Manager who will provide training, support, and oversight of the program operations; and 3) support from our 24-hour a day monitoring center who can assist with technical support for alert information on participants, trouble-shooting, and assistance with reports. Our proposed equipment does not pose a safety or health threat to the wearer or unduly restrict the activities of the participant. Additionally, our equipment includes a hypoallergenic design to reduce any discomfort in wear to the participant. All of Sentinel's proposed equipment has been properly registered and certified under Federal Communications Commission (FCC) rules and regulations.

The following provides a summary and highlights our proposed equipment offering for the Electronic Monitoring for Community Corrections program. Please note, under proposal section **4. Scope of Work** (page 54) we have provided our response to the requirements contained within RFP.

3.5 RF Patrol Radio Frequency Electronic Monitoring Solution

Sentinel is pleased to propose the latest in radio frequency (RF) technology, our RF Patrol Radio Frequency (RF) electronic monitoring technology. RF Patrol is designed to determine whether or not a participant remains within a preset distance from the home monitoring unit located in their residence using a small, lightweight bracelet that is designed to be installed on the ankle of the participant. This equipment is capable of continuously signaling, receiving, storing, and disseminating data (through landline or cellular communications) generated by the system to the Sentinel monitoring center, all without any active involvement by the participant.

RF Patrol is specifically designed for house arrest monitoring and provides more reliable home supervision and intensive heightened notification including unauthorized absences, late returns, equipment malfunctions and tamper alerts.

The two (2) elements of the highly advanced and secure system known as RF Patrol include the following:

+ PTX2: Bracelet ("transmitter") (page 16); and
+ PHMU: Personal Home Monitoring Unit ("home unit") (page 18).

3.5.1 RF Patrol Bracelet (PTX2 or "Transmitter")

The RF Patrol transmitter (PTX2) is 1.57 X 2.72 X 0.77 inches and weighs 1.51 ounces. The unobtrusive, hypoallergenic and sleek bracelet design makes it one *of the smallest body-worn bracelets available on the market*. It is easily, securely and comfortably attached to the ankle of participants under normal slacks. It is moisture and waterproof, shock resistant, unaffected by normal human environmental and atmospheric conditions, and does not pose a safety or health threat to the wearer or unduly restrict the activities of the participant.

RF PATROL BRACELET (PTX2)

RF Patrol will detect and store with a date and time stamp the low battery condition of the bracelet and the receiver. The bracelet 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, proactively replaced by Sentinel at an 18-month interval and has a four (4) year shelf life. The RF Patrol bracelet 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.

The RF Patrol PTX2 transmitter emits a unique, constantly changing signal *on average three (3) times per minute*. Each time the bracelet transmits its signal, it reports the serial number of the transmitter associated to the participant, its power status and tamper status.

—IMPORTANT SENTINEL ADVANTAGE—
The bracelet records and reports each tamper as a separate event alerting the agency of a participant's tamper frequency level. The RF Patrol monitoring system's signal range is agency programmable and variable with three (3) settings as follows:

- Low, approximately 50 feet
- Medium, approximately 100 feet
- High, approximately 150 feet

Additionally, RF Patrol has one of the shortest departure "leave windows" in the industry, allowing RF Patrol to report departures and arrivals quickly and accurately.

To prevent interference, tracing or duplication of the radio frequency signal, the RF Patrol bracelet signal has a 24-bit data string with more than four (4) million unique combinations. This design prohibits duplicates 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 bracelet signal features a patented circuit and is designed to discourage tracing or duplicating by automatically and constantly changing the transmitter transmission pulse rates (unique to each bracelet) during every other pulse to provide added protection against signal duplication and/or frequency interference.
- **Encrypted Radio Transmissions:** The RF Patrol bracelet uses more than *four (4) million* unique transmission combinations. The constantly changing pulse rate is unique for each active bracelet, making it virtually impossible to predict or duplicate through the use of counterfeit transmitters or other radio equipment. The home unit is aware and anticipates how each specific bracelet will vary transmissions. *No other electronic monitoring companies have incorporated this intelligence into their radio frequency monitoring systems units or devices.*

3.5.2 Tamper Detection – Fiber Optic Strap

RF Patrol has a highly-advanced tamper detection scheme. Sentinel was the first to introduce its sophisticated fiber-optic strap design that 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. If a participant attempts to cut the fiber-optic strap or remove the unit, the unit automatically activates a "tamper alert" signal and transmits the "tamper alert" to the home monitoring unit on an average of approximately once every 18 seconds while in range. Sentinel bracelets 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.

Sentinel provides straps designed to fit any ankle size. When properly installed, participants cannot remove the bracelet without destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot stretch or slip off the bracelet 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 bracelet, and then reset the bracelet once the band is secure. A visual inspection produces a "Restart" event for the PTX2 transmitter, confirming that an authorized person has manually reset the device.

3.5.3 Landline and Cellular-Enabled RF Patrol Home Monitoring Unit (PHMU or "Home Unit")

The RF Patrol home unit is 7.5 x 8.6 x 1.7 inches and weighs less than one (1) pound, making it one (1) of the smallest devices on the market capable of storage at 100% humidity. The RF Patrol home unit operates properly in households containing normal household goods and appliances. The RF Patrol PHMU is installed in a central location, using a standard two-prong 110-volt AC power cord certified to Underwriters Laboratories (UL) standards. The home unit also has internal surge protectors for the power supply and cellular modem incorporated into the internal architecture. The RF Patrol Cellular PHMU uses the GSM Network to communicate and transmit monitoring data to the monitoring center. *Home units are* available *in both Landline and Cellular to accommodate all participants,* even those without home phone lines and/or those that live in areas were cellular service may be limited. All communications between the PHMU (both landline and cellular units) and the monitoring center are sent through Sentinel's 800 toll-free number so there is no additional charge to the agency or program participant. 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.

RF PATROL HOME MONITORING

The RF Patrol PHMU is designed with a built-in auto-recharging backup battery that functions for up to 48 continuous hours of full operation (including but not limited to detecting and reporting information) in the event of a commercial power failure at the participant's home or power cord disconnection. Additionally, the PHMU will produce a red front panel indicator light to encourage the participant or other persons in the home to ensure the unit is properly plugged in and to reconnect the PHMU power cable if he or she discovers a problem. Despite the reason for power outage, the built-in back-up battery will provide full operation (including dialing and reporting) during continuous power outages for up to 48 hours. Receivers of some other manufacturers do not offer complete operation until 110-volt AC power is restored, dramatically impacting response times for notification. This feature is particularly important to agencies that do not have weekend and/or holiday officer coverage to respond to exceptions. Sentinel's monitoring application can notify the agency immediately each time there is a power outage or restoration of power.

—IMPORTANT SENTINEL ADVANTAGE—

In the unlikely event that a power outage exceeds the 48-hour battery back-up and is forced to shut down prior to reporting any event, the RF Patrol PHMU has an internal non-volatile memory capable of indefinitely storing approximately 90 days of monitoring events, including date and time stamps. The unit retains all stored events and reports them to the monitoring center upon power restoration and in cases where cellular units are being used restoration of cellular connectivity.

Upon activation, the home unit automatically identifies the PTX2 transmitter serial number assigned to it and synchronizes itself and the bracelet as a matched set. The transmitter and home unit are also interchangeable components, enabling easy replacement of either component without replacement of the entire system. *In addition, any home unit can be programmed to recognize and report statuses from multiple bracelet units (up to 50 transmitters on one (1) home unit),* including multiple participants in the same home and guest bracelets in the vicinity of the home unit.

—IMPORTANT SENTINEL ADVANTAGE / VALUE-ADD—

Some unique features of RF Patrol include:

+ RF Patrol has one of the shortest standard departure "leave windows" in the industry with a default five-minute leave window without producing false leave signals, allowing *RF Patrol* to report departures and arrivals faster and more accurately that any other vendor on the market.
+ The PTX2 is one of the smallest body-attached bracelets on the market
+ The PHMU is available in both landline and cellular to accommodate all participants, even those without home phone lines.
+ The RF Patrol Cellular PHMU uses either the AT&T or T-Mobile cellular network for communicating with Sentinel's monitoring system.
+ **Guest Bracelet Detection**
  The system detects all PTX2 bracelets that come within range of the PHMU. This unique feature detects if EM participants come in contact with one another and/or are comingling.
+ **Group Monitoring Capabilities**
  One (1) PHMU can simultaneously monitor up to 50 PTX2s.
+ **Ease of Installation**
  Officers can enroll the PHMU before or after the PTX2 is on the participant. Installers can complete PHMU enrollment through easy to follow prompts on the LCD screen in the office or at the participant's home. A telephone line is not required to complete the enrollment process.
+ **Advanced Range Testing/Variable Range Setting**
  Both the PTX2 bracelet and the PHMU indicate RF signal strength during range testing. This enables staff to perform accurate range testing at each installation and the officer can also determine the distance of the range setting in one of multiple distance settings.
+ **Unauthorized Telephone Number Reporting**
  The system will detect and report if a PHMU calls in from an unauthorized telephone number, including delivery of that unauthorized phone number to local personnel.

+ **LCD Screen**
  Provides alphanumeric informational prompts to local personnel during installation, troubleshooting and monitoring status through the Setup Menu options.
+ **LED Lights**
  LED lights provide a clear indication of connection and/or pending alerts to assist during programming or troubleshooting.
+ **Menu Options Reporting**
  The PHMU records and reports any time its menu options have been accessed.
+ **Ease of Termination of Service**
  Simple decommission procedures offer a variety of methods to power down one (1) or both devices.
+ **Bracelet Battery Level Indicator**
  Sentinel's PTX2 is the only bracelet on the market that continuously reports the remaining battery life to the Personal Home Monitoring Unit (PHMU) making it visible to installers on the Liquid Crystal Display (LCD) of the PHMU. This unique feature enables local personnel to best match PTX2 remaining battery life with each participant's anticipated term on EM at the time of initial installation, thereby proactively mitigating service calls due to bracelet battery depletion during the participant's term.

PHMU DISPLAYING A PTX BATTERY LIFE OF 97.1% OR 535.3 DAYS REMAINING

+ The RF Patrol PTX2 transmitter emits a unique, constantly changing signal on average three (3) times per minute. Each time the bracelet transmits its signal, it reports the serial number of the transmitter associated to the participant, its power status and tamper status.
+ RF Patrol's signal range is agency programmable and variable with three (3) settings as follows:
  - Low, approximately 50 feet
  - Medium, approximately 100 feet
  - High, approximately 150 feet

RF PATROL PHMU LED DISPLAY FOR RANGE SETTING

3.5.4 Tamper Detection via Fiber Optic Strap

RF Patrol has a highly advanced tamper detection scheme. Sentinel was the first to introduce its sophisticated fiber-optic strap design that 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 confirming the status of the strap. If a participant attempts to cut the fiber-optic strap or remove the unit, the unit automatically activates a "tamper alert" signal and transmits the "tamper alert" to the home monitoring unit on an average of approximately three (3) times per minute while in range. Sentinel bracelets 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 potential of "false tamper" alerts created through normal usage at home or in typical work environments.

Sentinel provides straps designed to fit any ankle size. When properly installed, participants cannot remove the bracelet without destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot stretch or slip off the bracelet 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 bracelet, and then reset the bracelet once the band is secure. A visual inspection produces a "Restart" event for the PTX2 transmitter, confirming that an authorized person has manually reset the device.

RF PATROL PHMU LED DISPLAY
BAND CLOSE CONFIRMED

3.6 OM400 One-Piece GPS Tracking Solution

Sentinel's proposed complete turnkey GPS Monitoring Equipment and Services solution includes the use of our field-tested and proven latest generation OM400™ GPS device capable of providing Active, Hybrid, and Passive tracking service levels. The OM400 GPS device being offered herein continues to be the one-piece GPS product of choice by those agencies who have conducted field testing of multiple GPS devices prior to making an award. The OM400 GPS device is both the receiver of location information and the transmitter of status and location information and is supported by an innovative, user-friendly web-based information exchange. The OM400 is a one-piece single body worn device that does not require a base or docking station, or landline communications.

The location-based monitoring equipment offered by Sentinel is unique from other GPS offender tracking devices in that Sentinel's proposed device uses both GPS and Advanced Forward Link Trilateration (AFLT) technologies to track offenders' locations. This dual-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking.


OM400 MONITORING DEVICE

The OM400 GPS device also has multiple unique, state-of-the-art features that make it a valuable supervision tool including:

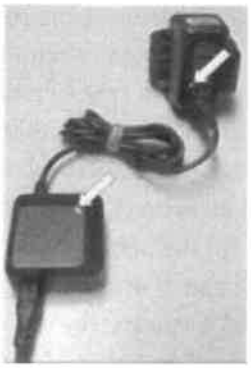
+ One-piece device that provides up to three days (72 hours) of continuous operation on a single charge.
+ GPS Yield Improvement that maintains near 100% GPS yield for all operating modes for both outdoor and indoor monitoring (optional beacon where needed; see below for details).
+ Alerts right from the home screen, including active alerts and battery level.
+ Display of multiple sub-companies without having to log on and off.
+ Offender communication through vibration or beeping the device.

- Offender acknowledgement of communication by depressing the button located on the front of the device.
- Zones stored on board the device in order to provide immediate notification on zone violations.
- Track Location/Pursuit Mode providing the ability to increase the GPS location capture to one (1) point every 30 seconds and transmitting every 60 seconds.
- Tag or clear an alert and add notes.
- Current location requests with access to navigate to maps to get turn-by-turn directions.
- Display photo of offender with case/profile information.
- New mapping features that allow users to receive more information about location data, including the speed of travel, the type of location point, and the number of satellites that were in view at the time the point was generated.
- Verizon and Sprint are the primary cellular communications networks and the device roams on all other CDMA networks as needed.

3.6.1 Overview of the OM400 Device

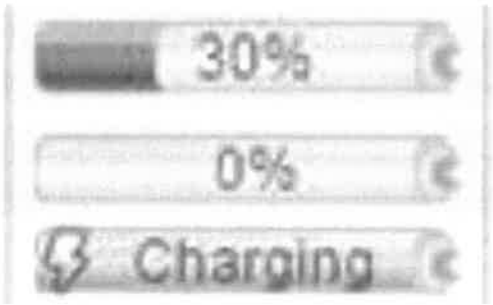
The OM400 is a discrete unit that is easily, securely and comfortably attached to the ankle of the participant. The OM400 tracking device is a one-piece device that is FCC certified (FCC ID AB3-OM400) and is small and light weight with the device's dimensions at approximately 3.5 x 2.4 x 1.6 inches and weighing 8.4 ounces. The OM400 device casing is hardened and waterproof in both salt water and fresh water. The unit can withstand temperatures between -68° Fahrenheit and 155° Fahrenheit, humidity of less than 95 percent, normal household and atmospheric conditions, and up to 500 MHz of random vibration of 1.25G rms. The unit is also dishwasher safe, which is the easiest and most effective way to sterilize the device.

The OM400 features an internal battery that boasts one of the industry's longest battery lives of 12 to 18 months with a shelf life of three (3) years. Participants charge the unit through a standard 110V plug with a 15-foot cord easily connected directly to the front of the unit. The unit has an intensive monitoring battery life of up to 72 hours depending upon the rate plan used by the agency and is rechargeable in 1.5 hours. The OM400 features a multi-colored LED light that will illuminate during battery charging.



OM SERIES LED LIGHTS

Additionally, the device reports the battery status each time it reports to the monitoring center. If the device's power is low, the monitoring center will generate a low battery alert. A low battery alert is generally generated when the device is at 20% or less of battery power. This alert will clear when battery power is restored above 85%. To mitigate low battery issues, agencies can incorporate a mandatory recharging schedule into the participant's daily schedule. If the device is not charging at the scheduled time, or if it is unplugged prior to the expiration of the charging schedule, the monitoring center can notify staff if required. The software also allows the agency to require the OM400 device to take specific action such as vibrating to alert the participant in the event of a low battery.

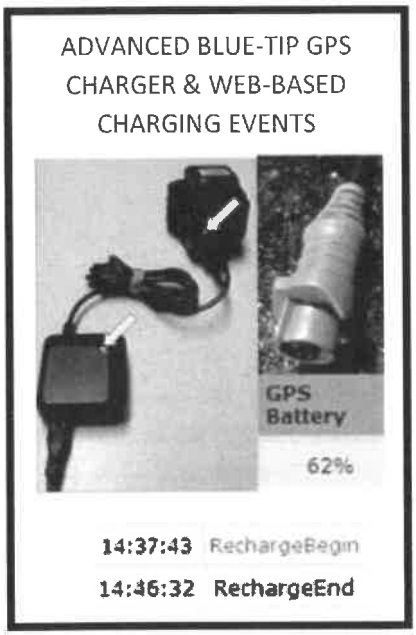


OM SERIES BATTERY STATUS

The device is extremely easy to attach to the participant's ankle with a reusable, adjustable and replaceable strap. The strap includes a permanently embedded fiber-optic cable and is fully adjustable, eliminating the need for strap cutting during installation. Two (2) locking pins connect the unit to the back plate. Personnel installing an OM400 GPS tracking device on the participant need *no tools*. Our staff will connect the device to the ankle of the participant with only their thumb and forefinger. Once properly attached, the device will detect and report a tamper message if it is removed. The OM400 GPS tracking device strap is easily sanitized and reusable on multiple participants without the need for replacement. The device is attached to the participant's ankle with an extended length band to accommodate the largest of ankles. The strap's design allows for a secure fit and has multiple holes to assist in finding the proper fit on each person. The strap is adjustable as needed prior to locking the pins in place to allow the participant to stand up and/or walk around to determine the best fit possible.

The OM400 GPS tracking device's unique design will allow the agency complete confidence that the device installation is successful. Sentinel staff will enroll the participant in the monitoring system application. The enrollment process is quick, simple and completed in five (5) to 10 minutes by entering basic data and selecting the respective officer. Upon a participant's enrollment, the installer will fit a sanitized unit on the participant through a straightforward configuration process which consists of 1) adjusting the strap to the participant's ankle, 2) securing the device on the participant, 3) changing the status of the device to active and 4) assigning the device to the participant on the web-based platform. The software recognizes the device as soon as it is activated and assigned to the participant, providing confirmation that the device is working properly.

—IMPORTANT SENTINEL ADVANTAGE—
Sentinel recently introduced and recently began deploying an *advanced blue-tip GPS charger for improved connectivity, longer life, and increased durability.* See image to the right for an example of the blue-tip chargers.



3.6.2 Tamper Detection Features

The OM400 GPS tracking device detects three (3) tamper types including 1) strap tamper, 2) device case tamper and 3) backplate tamper. Within one (1) second of a tamper attempt, the device will communicate and send a unique alert to the monitoring system web interface. *The OM400 device will automatically and instantly communicate to the monitoring system software when a participant attempts to remove or tamper with the strap.* The monitoring system then immediately sends the alert to the appropriate personnel. The OM400 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the back plate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit.

When properly installed, attempts to defeat, remove or tamper with the OM400 GPS tracking device will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The back plate fits precisely in place and any attempts to pry it open are easily noticeable.

The OM400 devices offer the most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. The devices remain in tamper until inspected and reset through the monitoring system software. This process eliminates nuisance tamper events reduces tampers to only those that truly warrant investigation and necessitate oversight. Sentinel's on-site staff can utilize any internet enabled device to access the software in order to clear a tamper, or they can call Sentinel's national monitoring center to clear the tamper event for them. A mobile application is also available to allow our staff to clear alerts or access participant activity when away from the office.

3.6.3 Multiple Modes of Operation Programmable Through the Web-Based Monitoring Application

The OM400 unit is both the transmitter and receiver of information in one (1) unit and is equipped with on-board processing capabilities. The unit will track at one (1) point per minute and store several days of tracking information in the on-board memory, regardless of the mode of operation, should the unit be unable to communicate with the monitoring application. The OM400 is also able to store zones on board the device in order to provide immediate notifications on zone alerts. Through the supporting monitoring software application, our proposed solution provides the flexibility needed for controlling the level of supervision each participant receives to meet individual monitoring demands. This level is defined by the type of monitoring assigned in the participant's profile. The profile not only defines the monitoring intensity, but also allows our staff to change the level as directed by the referring agency, based on a participant's current monitoring status. Profiles available include the ability to track on a minute-by-minute basis if desired. The most common profiles are identified below but may be customized to meet program requirements.

RISK PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point either in 60 second increments and transmits data every 10 minutes and includes an Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every 60 seconds and transmits data every 30 minutes and includes an Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every 60 seconds and transmits data every 60 minutes and includes an Impaired Locate every 60 minutes. Tampers and zone violations are immediately transmitted.	Less risky participants requiring only strong supervision

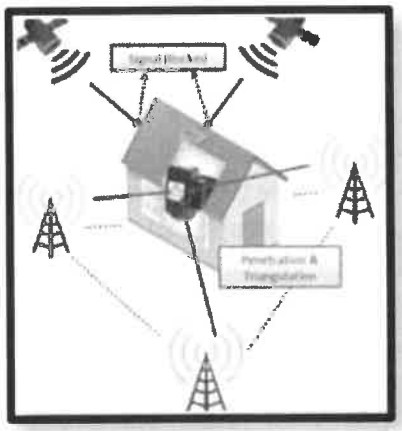
The monitoring application allows our staff to set up advanced warning parameters in order to create buffer zones around exclusion zones to alert individuals of an upcoming potential violation of the zone.

Buffer zones provide an extra layer of security around exclusion zone borders, and enhance notifications and rapid response to exclusion zone violations. A buffer zone is an extended area surrounding an exclusion zone. Once the buffer zone is breached, a Buffer Zone Alert is generated and the device increases its GPS acquisition and cellular transmission rate to real-time tracking: 1 minute by 1 minute. This puts monitoring personnel on alert and allows for early intervention before the exclusion zone is breached. Tracking will continue in real-time to provide the fastest possible notification on proximity to the exclusion zone until the participant has cleared the area.

Mobile Exclusion Zones (MEZ) allow agencies to ensure that a participant on monitoring does not come near another specific individual anywhere they may be. Taking monitoring beyond stationary zones, the MEZ program monitors the activity of two GPS devices to determine their proximity from one another in the real world. Often used for victim protection and in domestic violence cases, the victim carries a

device while the participant wears one. If the two devices come within a specified distance of each other, notifications are generated and law enforcement may be contacted. The victim may also be notified, giving her necessary information to help her find safety.

3.6.4 Secondary Location Tracking Features



The OM400 uses both GPS and Advanced Forward Link Trilateration (AFLT) technologies to track offenders' locations. This dual-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking.

The OM400 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM400's unique design combines multiple layers of location technologies including AFLT (Advanced Forward Link Trilateration), GPS, and Assisted GPS (A-GPS). Such technology allows for reliable location information to be processed anywhere and compensate for poor GPS availability in GPS-impaired environments. The combination on these advanced location technologies allows for the quickest acquisition time (typically within 60 seconds, so long as there a cellular signal detected) without an office being required to go outside to acquire a GPS signal when enrolling and installing a device.

The OM400 acquires GPS utilizing a system of satellites signals and, in the event the OM400 can only find a few GPS satellite signals due to partial blockage or location, it willautomatically shift to A-GPS. With A-GPS, the OM400 uses the available GPS signals in combination with cellular network data. In the instance of impaired GPS, or no GPS signal, the OM400 activates Advanced Forward Link Trilateration (AFLT). The AFLT triangulates utilizing ambient longitude and latitude data broadcast by the cellular environment. This is a unique capability and is possible with devices communicating via a CDMA cellular network.

The OM400 communicates via the **Verizon or Sprint** networks, both CDMA-based. Designed to track and allow communication with the offender 24/7, the OM400 locates indoors and out. As with typical GPS, interference is a reality and in any case, there are two (2) formats of signal that can be impacted; GPS and cellular signal. Such obstacles are geographic in nature (poor GPS location), signal disruptors (scramblers, shielding, tracing, and duplication), cellular turndown (termination of many 2G GSM networks as announced by AT&T), and locations with poor cellular reception. Taking these obstacles in mind, the OM400 technology is centered on reliably offering two (2) cellular networks - Verizon and Sprint - to heighten cellular options and provide reliable location data in GPS-impaired locations. The OM400 uses the CDMA wireless digital cellular standard to transmit and communicate data directly to the monitoring system via two (2) of the largest cellular networks in the world. The OM400 device uses encrypted communications that prevents tracing and duplication. Additionally, the OM400, through its CDMA communication capabilities, is not subject to the eminent, and in some cases immediate,

"turndown of service" that has been announced by major GSM networks like AT&T. Therefore, there is no threat of interruption of service.

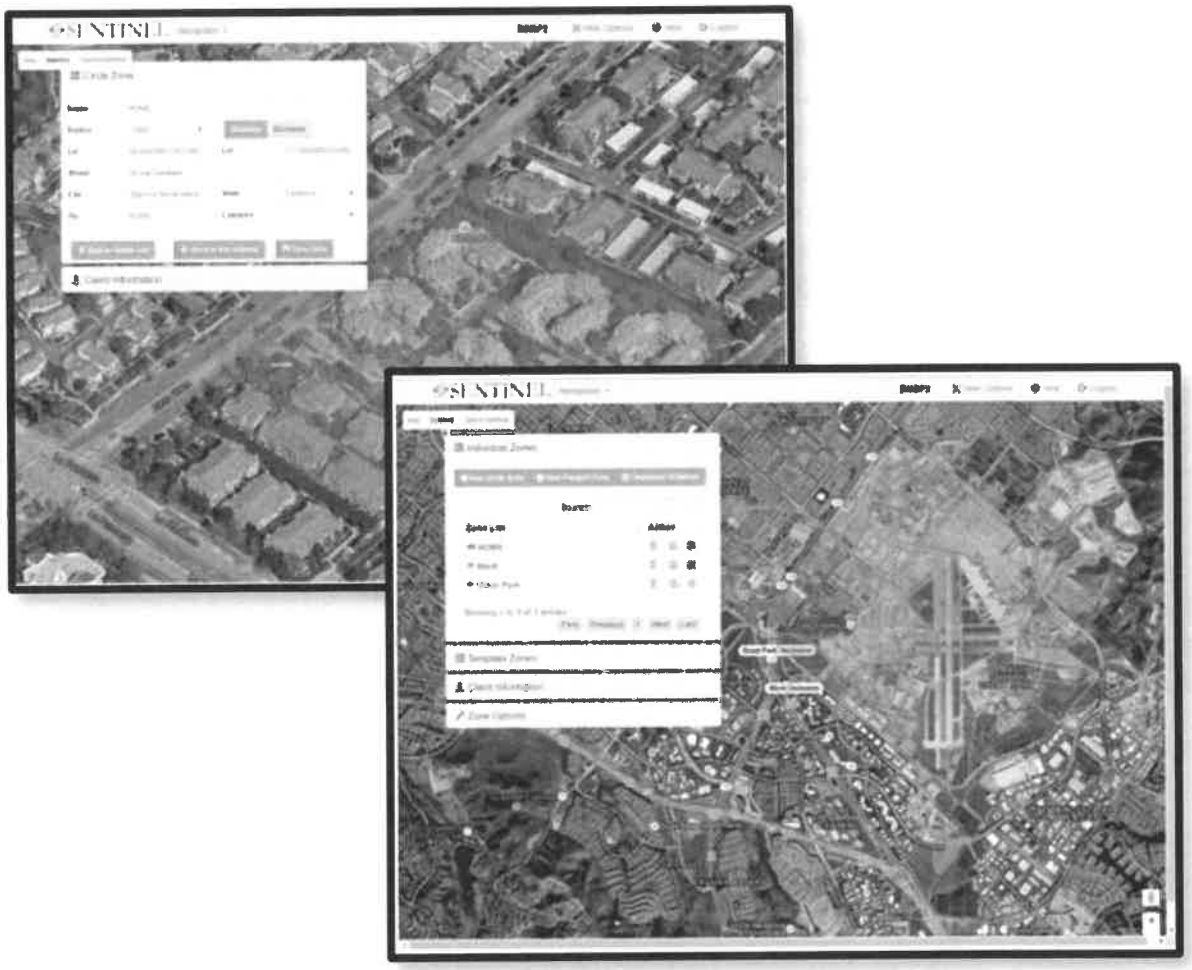
All GPS manufacturers utilize the same government satellites; therefore, all GPS leading systems are comparable in accuracy terms as the accuracy is directly related to the number of satellites that are being received by the GPS receiver; the more satellites the more accurate the positioning fix. The accuracy could roughly be broken out as shown in the following table:

NUMBER OF SATELLITES	DEGREE OF ACCURACY
1 - 2 satellites	No fix can be established
3 - 4 satellites	30-meter accuracy
4 - 6 satellites	10 - 30-meter accuracy
7 - 9 satellites	3 - 10-meter accuracy
10 or more	Better than 3-meter accuracy

GPS accuracy can vary with any GPS manufacturer based on the satellite reception at any given point therefore it is important for officer's to be able to promptly determine the accuracy of any tracking point in order to determine the basis for compliance and/or potential violation. The AFLT may enable tracking in such impaired locations with a point accuracy of better than 30 feet.

3.6.5 Creating Schedules and Zones (Inclusion, Exclusion, and Buffer)

An important feature of the Sentinel-proposed monitoring software application is the ability to develop zones. Authorized staff will have the ability to create inclusion zones that are geographic areas where an offender is scheduled to be, such as home or work; they will also have the ability to create exclusion zones, which are geographic areas where the offender is not permitted to visit such as a victim's home, schools, or areas outside the state or county border. In addition, the proposed monitoring software application provides the ability to configure zones in the shapes of circles, rectangles, and arbitrarily shaped polygons, as well as be able to have zones within zones.



Zones can be created as offender zones, if only one offender will need to use the zone, and company zones that can be created and stored within the system as a library of zones in the event there are multiple offenders who need to use the same zone. Some examples of company zones include schools, parks, and/or day care centers. Authorized staff will be able to create groups of company zones that can be assigned or unassigned from the group and a schedule for the group zones can be created with a single entry.

—IMPORTANT SENTINEL ADVANTAGE—

Authorized staff have the ability to upload circular and rectangular zones to the device in order to generate immediate notifications when a zone is crossed. This capability allows for near real-time alert notifications and processing. The agency will have the ability to designate which circular and/or rectangular zones they would like uploaded to the device to allow for those immediate notifications and processing by the monitoring center.

3.6.5.1 Scheduled Zones

The web-based monitoring software application includes a participant's schedule tab that will allow your staff to associate participants and zones with times of the day. County personnel will be able to easily create schedules to control which zones an offender can enter during specific times of the day. For example, if a participant is supposed to be at home at night, then a schedule can be established to ensure that he/she does not leave the "home" zone during certain hours. If a participant should be at work during the day, a schedule can be established to make sure he/she is at work, and not somewhere else. The software application will also allow our staff to create a schedule to specify when the GPS device's battery should be charged.

3.6.5.2 Mobile Zones and Buffer Zones

The OM400 and the monitoring software application also offer the ability to create Mobile Zones and Buffer Zones to maximize the effectiveness of the program. The solution provides not only the ability to create an exclusion zone around a victim's home or work place, but also around the victim themselves via a Mobile Exclusion Zone. This is done through a secondary tracking device voluntarily carried by the victim thereby providing additional alerts when the offender breaches the victim's mobile zone. Buffer Zones allow for early detection for potential violations by enabling us to establish an additional perimeter around a zone (any size) that will alert when the offender has breached the buffer zone prior to their entering the exclusion zone.

3.6.5.3 Additional Zoning Features

Further zoning features include:

+ Unlimited zones are possible on the software for immediate analysis.
+ Customized schedules can be created for any offender around inclusion zones and exclusion zones.
+ The system boasts a robust and user-friendly scheduling and zone creation system offering various zone forms from circular, polygon, custom free-form drawn zones, even to zoned routes, providing the ability to maximize restrictions.
+ Users are given the ability to create route/travel zones allowing for optimized restriction and supervision of offenders down to daily commutes.
+ Users have the ability to create zones around people. These can be mobile exclusion zones around a victim's device or another offender's device. The size of the zone is determined by the referring agency.
+ Ability to create zones around fixed locations. These can be inclusion zones (places an offender has to be), exclusion zones (places an offender should not be) and undifferentiated zones – for notification of entry and exit without scheduled rules associated. On the map Inclusion Zones are green and Exclusion Zones are red. They can overlap and change based on designated times. For example, a person may have to stay in the City of Lexington (Inclusion Zone) but not be allowed near the victim's house (Exclusion Zone) except during a 1-hour period to pick up children (Inclusion or Undifferentiated Zone).

- Zones can switch during the day – for juveniles, for instance, the person must be on campus during school hours, and must not be there after hours – the zone would switch from a green inclusion zone to a red exclusion zone
- Advanced warning parameters enabled to create buffer zones around fixed or mobile exclusion zones to alert individuals and/or victims of an upcoming potential violation of a zone.

3.7 BA/RT - Breath Alcohol / Real-Time - Monitoring Solution

Sentinel is proposing our latest addition to alcohol monitoring, Breath Alcohol / Real Time (BA/RT), to provide participants with portable handheld remote breath alcohol monitoring equipment. BA/RT provides random, scheduled, and on-demand testing, which is available and configurable through our web-based monitoring platform. The unit is a portable, lightweight, handheld device that brings the latest in alcohol monitoring technology to criminal justice agencies nationwide.

3.7.1 Overview of the BA/RT Unit

BA/RT is non-invasive and equipped with a state-of-the-art deep lung fuel cell sensor that will provide the agency with reliable and true BrAC readings that are based on definitive data. Further, in order to determine the breath alcohol concentration (in a breath "per se" state) and thus the level of intoxication, it is imperative that the body temperature is known at the time of the participant test in order to guarantee that the breath sample is human. Therefore, during each participant test, BA/RT also incorporates a measurement of breath temperature and it is reported along with the BrAC. The addition of the measurement of the breath temperature during each breath test makes the BA/RT system a highly accurate means of determining the level of intoxication and reduces the potential of a participant's attorney challenging the results; in addition to a photo taken during the time of the test, detecting temperature and humidity is an additional level of security to ensure the participant is the actual person taking the test and a valid breath sample is submitted.

The BA/RT device is 6" long, 2.4" wide, and 1.4" thick with a weight of approximately 6.8 ounces. This device is designed to be easy to carry at all times by the participant in a Sentinel-provided protective pouch that protects the unit and allows the plastic mouthpieces to remain with the unit at all times. The BA/RT device is made of impact-resistant, non-flammable, injection-molded plastic. The unit is designed with rounded-edges and encased in drop-resistant ABS plastic with a rubber protection band for added security from accidental/incidental damage.

The BA/RT unit features a rechargeable 1800 MAH battery that will provide in excess of one day of continuous power to the unit while the participant is out in the community. The unit is easily recharged in approximately one hour through its USB charging port found on the bottom of the device with a standard portable wall charger (similar to a cell phone charger). The unit will check-in to the Sentinel monitoring center a minimum of once every 45 minutes to ensure the proper operation and adequate battery life of the device. When the battery condition reaches a pre-determined level of depletion, the unit will initiate an audible tone every minute, display "CHARGE BATTERY NOW" on the LCD display and the red LED will slowly blink. The audible beep is a progressive feature and will begin beeping more rapidly after one (1) hour and the unit will automatically report the low battery status to the monitoring center after two (2) hours for further resolution procedures.

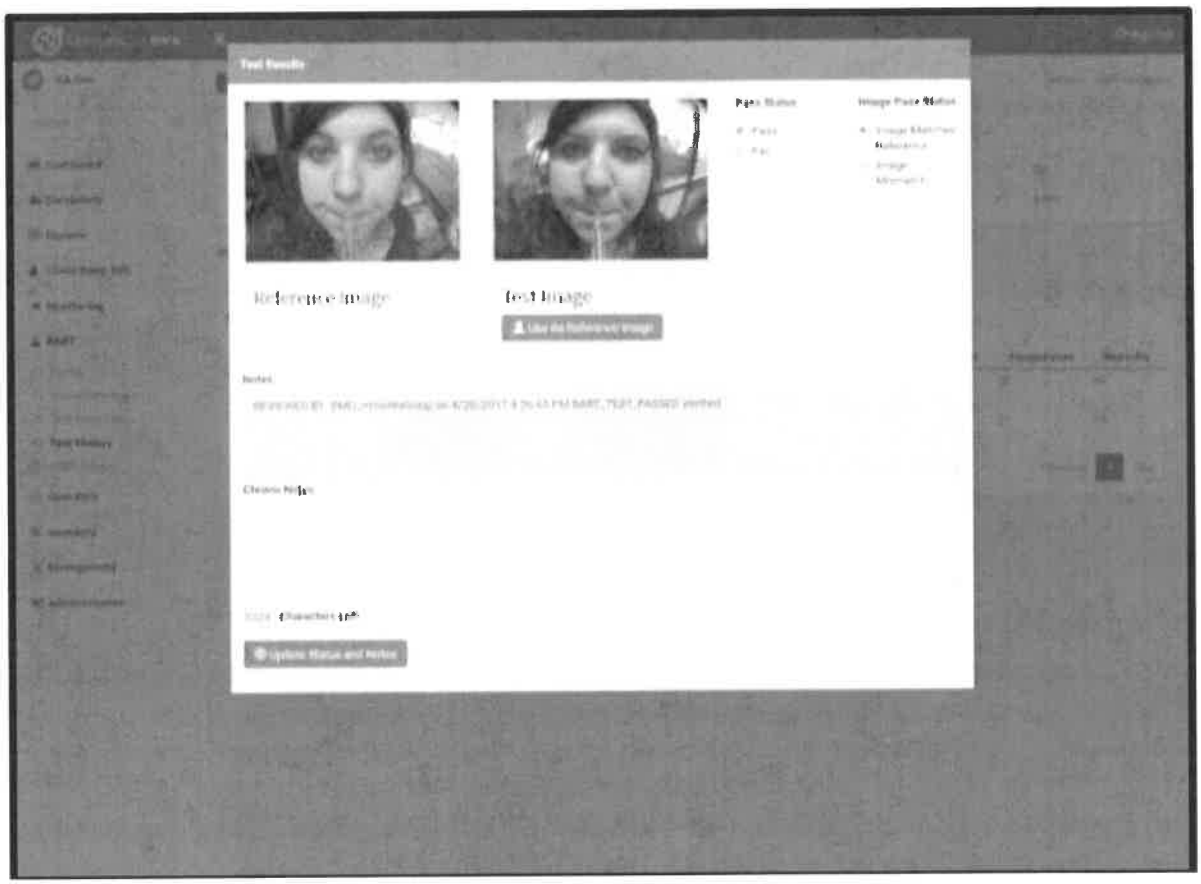
BA/RT MONITORING SOLUTION

3.7.2 Alcohol Testing Protocols

When it is time for a test, BA/RT delivers an audible and visual signal, reducing the risk of a missed test. It then guides the participant through testing via alphanumeric display prompts and multiple colored LEDs. BA/RT determines its location during testing using built-in GPS technologies and immediately transmits all data to our 24/7 Monitoring Center for notification processing by the Monitoring Center staff. Results are available immediately via our web-based information system, allowing agency staff immediate access to all monitoring data and to respond accordingly.

An added feature of BA/RT is the ability for officers to directly communicate with the participant. The message appears on BA/RT's high-resolution LED screen and the participant acknowledges receipt of the message. When it comes to enforcing alcohol abstinence orders, every minute counts and officers need the opportunity to react quickly. BA/RT makes this possible anywhere and at any time.

To ensure the integrity of each test, BA/RT is equipped with a built-in high-resolution camera that captures a color image of the participant as the test is being performed. Each test image is compared to the participant's master reference image to verify his or her identity. The following shows the reference picture taken at the time of enrollment versus the actual test image providing positive verification.



3.7.3 Unique / Advanced Features of the BA/RT Solution

The BA/RT unit is designed to provide portable, officer accessible, real-time alcohol testing of program participants. Tests can be on-demand, scheduled, or random and location information is sent with each test. BA/RT is fuel cell driven and takes a deep lung breath sample. The following list highlights some of the unique features of the proposed BA/RT portable alcohol monitoring system:

+ **Remote BrAC Testing:** Mobile handheld alcohol testing device capable of performing tests in any location as a participant travels throughout the community.
+ **Live Monitoring Staff Confirmation of Each Test:** Each alcohol monitoring test result and picture is reviewed and analyzed by a live operator to ensure positive identification of the participant being tested.
+ **Breath Temperature/Humidity:** In order to determine the breath alcohol concentration (in a breath "per se" state) and thus the level of intoxication, BA/RT reports the breath temperature and humidity at the time of each test. This is also used to ensure that it is actual human breath being sampled when taking the test. This feature provides added security and reliability over any other Breath Alcohol Testing device being proposed by other providers.
+ **Cellular Reporting Capability:** BA/RT features immediate reporting of alcohol test results via the CDMA cellular network (no home phone line needed).

- **Extensive Memory:** On-board memory can store as many as 1,500 tests in the event of temporary cellular signal loss and includes date and time stamp of each stored event (Note: The unit will automatically initiate a call-in when it detects the restoration of cellular connectivity).
- **One-Piece of Equipment:** Requires no body-worn equipment or no home-based equipment meaning there is no need for the participant to maintain a home phone line or installers to go to the participant's home to complete enrollment.
- **Battery Life Awareness:** Low battery notification through audible alert, LED lights and LCD display when the device reaches its battery life alert threshold.
- **Proven Breath Testing Technology:** Deep lung sample tested through proven fuel cell technology to provide accurate numeric BAC (example 0.123) to the supervising agency.
- **Color Photo Participant Identification:** High resolution camera and front panel lights to provide color image of the participant during each test.
- **Web-based Scheduling:** Random, scheduled, and on-demand testing available and configurable through web-based monitoring platform.
- **Participant Location Identification:** BA/RT provides location-based tracking of participant at the time of each test through GPS. The BA/RT unit can be used in conjunction with a Radio Frequency or GPS program as well as a standalone breath alcohol testing unit.
- **Text Message Capability:** Agency to participant text communication capability on BA/RT LCD display with participant acknowledgement.
- **Automatic Retest:** As part of our procedures, we will automatically initiate follow-up tests when an offender's sample exceeds the court-mandated BrAC threshold, a test is not completed successfully, or if the test is not taken at all. All of these non-compliant events would be reported to the court as required.

3.8 Monitoring Services Provided

Sentinel is committed to providing excellent customer service and support to the Division, and therefore, we staff our monitoring center with multiple over-lapping shifts, which allows us to have more than sufficient personnel available at key peak traffic times. All of our operators are trained in properly fielding inquiries and providing Sentinel and agency personnel with the most accurate and detailed explanations. To ensure that our operators are performing their customer service duties properly, all telephone calls into and out of the monitoring center are recorded for quality control and record review purposes.

Sentinel's monitoring center and monitoring center staff have years of experience successfully delivering complex notification protocols for optional Enhanced Notification, including but not limited to alcohol testing protocols whereby Monitoring Center Staff triage and escalate alerts and/or troubleshoot alerts, calling/texting participants on home/mobile phones, calling/texting/emailing officers at office/on mobile, calling/triaging locally-based Sentinel installers for local services, and documenting results within Sentinel's web-based system.

Sentinel will provide services in compliance with all of the Electronic Monitoring for Community Corrections program requirements. In addition, Sentinel offers the following:

+ Calling offenders directly when a key event occurs, following the protocol for that key event, and the agency-defined script
+ Entering comments or event information for each alert that occurs in the offender's monitoring record
+ Initiating contact procedures in the event of an emergency
+ Receiving calls from both local Sentinel staff and agency personnel as required, and update case notes as required

Our immediate interaction when processing alerts is geared towards being able to provide the referring agency's staff with as much event information as possible. This gives everyone the ability to reply more quickly since they have preliminary information on the alert that was delivered by the Sentinel operators. The goal is to have an alert notification procedure based on only sending the required information and not to burden anyone with non-critical signals.

Sentinel strives to resolve all inquiries promptly and on the first contact. Each monitoring center operator has the expertise to easily identify, explain and resolve issues relating to program needs such as assisting our local staff with 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.

As an additional enhancement to Sentinel's 24 hour a day support services, Sentinel provides an additional team of support staff delivering specialized services. This specialized Help Desk 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. Also, all calls are recorded and can be reviewed and made available to the Division as needed.

In addition, this specialized support services department performs testing of critical or on-going events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and pro-actively seeks to identify re-occurring issues to prevent problems that may 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 for the Regional Account Manager and local program staff for customer enhancement requests, suggestions and ideas.

3.9 Secure, Continuous Monitoring Center Operations

Our monitoring center is staffed 24 hours a day, seven (7) days a week with a supervisor on duty at all times and live operators cross-trained to support our suite of supervision services and products. We currently employ more than 70 staff members to staff our continuous operations (24/7) facility. This staffing allows agency staff to call and speak with one of our monitoring experts at all times of the day or night. We do not use a message delivery service; our operators answer all calls at all times. In addition, our center is staffed with bilingual personnel on every shift in order to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact offenders when certain alarms occur, regardless of the day of the week or time of the event.

Sentinel stores / archives for retrieval / backs up all monitoring data so that all authorized users with a computer and Internet browser (e.g., 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.

—IMPORTANT SENTINEL ADVANTAGE—
All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring center that is operational 24 hours a day, seven (7) days a week, 365 days a year.

The monitoring center is the focal point of Sentinel's state-of-the-art headquarters facility, located in Irvine, California, that is staffed 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls on a daily basis providing secure confidential monitoring services. The monitoring center is a separate, self-supporting node within the facility with is approximately 3,000 square feet and designed based on Underwriters Laboratory specifications. This is the central location from which all monitoring center activities are conducted, monitoring information is disseminated and technical support (help desk) services are provided.

Sentinel's proposed monitoring application is equipped with security features that prevent unauthorized individuals from accessing any information held by Sentinel. Secure access to the system is maintained at all times.

Sentinel's 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.

Sentinel uses an industry standard data protection and recovery software package to ensure that the databases within the primary and back-up data servers are concurrently maintained, which ensures the following:

+ No loss of data from the databases if there is a failover

+ Capability for the back-up database to immediately and automatically become available for processing and access

The system maintains a constant connection between the primary and back-up database servers and when it detects the loss of a regular "heartbeat" signal between the systems, it automatically initiates an alert notifying Sentinel of this loss. It is then determined if the loss of heartbeat was an anomaly or it is warrants a real-time failover from the primary database server to the back-up server. Regardless of the cause, Sentinel's contingency plans will failover in the case of any system malfunction that effects participant monitoring or reporting, which cannot be corrected immediately.

Additionally, access to Sentinel's web-based information exchange platform is automatically redirected to the back-up web server if there is a failure. 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.

Additionally, our monitoring system is only accessible to authorized personnel, with each user having a proprietary login and password. All changes to participant or demographic information and/or monitoring data are saved within the system. For quality control and security purposes, our Information Technology staff is able to view access trails left by users when they login into the system. This is used to conduct audits and Quality Control checks. Additionally, Sentinel's IT Department will provide any information on attempted intrusions or other relevant information to the agency for further investigation and referral for criminal action, should they occur.

3.9.1 Personnel Security

Only authorized personnel have access to offender data, and our monitoring center personnel are not allowed to modify any monitoring data. At no time will we 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 our employees are provided an employee handbook that outlines Sentinel's no tolerance policy regarding compromising relationships with participants, their families and/or customer staff. We will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the participating agency.

3.9.2 Security of Monitoring Records

To ensure that the proper information is entered at all times, our personnel are thoroughly trained on data entry procedures with supervisorial support for any adjustments or corrections. Each user is given their own login and once they set their confidential password, Sentinel can ensure the integrity of each user's entry. This unique user access allows our Information Technology personnel to follow electronic audit trails that allow supervisors and management to verify the source of all data entry.

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 alpha-numeric 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

NOTE: No offender data is stored on-board any field office workstation so that in the event, however unlikely, of remote component theft or destruction, confidential offender data and records will not be compromised. All data is stored securely at our monitoring center's secure super-server component configuration.

In addition, our monitoring center and secure web-based monitoring systems incorporate the latest in security measures. Due to the sensitive nature of the records that we handle daily, we have taken all possible precautions to ensure the integrity and security of its system. Protection of records and their confidentiality are our main concern. All of our security systems are monitored continuously to ensure no lapse in service.

3.9.3 Monitoring System Security

Our monitoring center is equipped with all of the latest systems to ensure its protection against any unauthorized access. 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. The system is backed up in its entirety every day with the data being stored off-site at a secure, private data storage facility.

All changes to participant or demographic information and/or monitoring data are saved within the system. Additionally, each 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 web-based information exchange architecture has internet servers that are independent and kept safe from primary data servers and computer systems. Our Information Technology staff has installed all of the necessary physical and technical security measures (*e.g.*, SSL certificates, network firewalls, anti-virus software, access control equipment, and closed-circuit television surveillance) to ensure that unauthorized users and hackers do not have access to Sentinel's information technology infrastructure, applications, or our national monitoring center facility.

3.9.4 Physical Security

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. For security purposes, the Irvine site does not conduct any business with the general public as it contains our corporate office and monitoring center. Program participants or monitored defendants have no access to this facility.

Our monitoring center is designed based on Underwriters Laboratory specifications and restricts access to authorized staff and our 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 (which we prevent through our previously described redundancy features)

The monitoring center is located on the second story of our Irvine corporate headquarters 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 steel-designed doors, authorized employees are issued electronic key cards that are the sole method of entry into the center. In addition, only authorized 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 our 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.

3.9.5 Disaster Mitigation

Sentinel's monitoring center has multiple disaster mitigation features, resides in an independently secured, climate-controlled facility with raised floors, has a fire suppression system, and written policies and procedures for access. The monitoring center meets all applicable federal, state and local regulations regarding safety including building codes regarding earthquake resistance and hurricane resistance.

Sentinel's proposed solution maintains physical security compliance with all applicable Federal, State and local regulations. Also, the proposed Monitoring Application runs on a secure, highly reliable, redundant, and scalable carrier-grade infrastructure. The proposed datacenter environment was designed with redundancy in mind at every layer. The platform is deployed at multiple datacenters to provide geographical redundancy. The infrastructure operates with high-availability storage area networks and database clustering. The datacenters are supervised by live hardware and software engineers 24/7/365 to ensure the best possible uptime, and are supported with five (5) local internet loop providers with redundancy for every switch and component. This infrastructure and system capability has manifested itself in the achievement of 99.999% uptime, as measured, graded, and reported by one of the top three (3) carriers in the United States. Also, the proposed Data Centers are certified by the following:

+ ISO9001
+ SAS-70 Audited
+ HIPPA certified

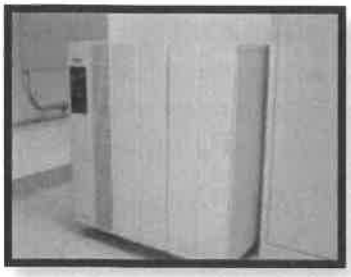
Data Center Security:

+ Four (4) physical layers of security
+ State-of-the-art access card system
+ Trained security personnel
+ Closed circuit television cameras (CCTV)
+ Biometric and Key Card secured facility
+ 24 hours a day, 7 days a week on-site staffing from dedicated security and storage engineers

The Data Center's electrical infrastructure consists of two (2) major components:

+ **A Distribution System**
  The distribution system has dedicated power sources that are provided by APS. The system is based on a redundant diverse distributed system consisting of Demarcation Power, Power Distribution Units (PDU), Uninterruptible Power Supplies (UPS) and a Utility Service Bus (USB). There are two (2) independent Utility Power Feeds on different sub-stations.

UNINTERRUPTIBLE POWER SUPPLY (UPS)



+ **An Emergency Power Generation System**
The emergency power generation system consists of Automatic Transfer Switches (ATS), Emergency Service Bus (ESB), and redundant diesel generation. The primary system has a redundant backup system rated at 100% of the capacity of the primary system. In the event of a power failure, the emergency diesel generators will provide power in less than 10 seconds and contain 1,000 hours of fuel for superior backup performance. Once started, the generator automatically ensures it is operating at sufficient capacity and then switches power from the grid to the generator. Data Center staff will conduct regular hourly inspections of the generator to ensure adequate fuel and proper operating parameters are maintained. The generator detects when the power grid resumes operation and within five (5) minutes restores power from the grid and shuts down the generator. This added redundancy virtually guarantees seamless and continuous power to the Data Center providing added confidence to the agency that public safety is ensured.

ON-SITE DIESEL GENERATOR

3.10 Sentinel's DNA Web-Based Monitoring and Tracking Platform

DNA is our state-of-the-art web-based monitoring and tracking software platform. Designed in-house by Sentinel software engineers, DNA can be customized to include all required reports, notification procedures and escalation alert sequencing. DNA will allow the RF Patrol electronic monitoring, OM400 GPS tracking and BA/RT breath alcohol monitoring technologies proposed herein to communicate on a single web accessible platform. Moreover, this powerful and easy to use platform will provide the Division with customizable features and benefits not available from other monitoring software solutions.

DNA makes it easy for officers to access real-time information about individual participants or on their caseload as a whole from a secure environment (user name and password are required for login). Designed with the needs of the end-user in mind, DNA uses a straightforward, intuitive user interface that allows users to complete all monitoring tasks including:

+ Enroll a participant
+ Create/edit curfew compliance schedules
+ View, create notes, clear event and alerts
+ Locate participants
+ Create and print reports
+ Perform case management administration
+ Create and edit zones (inclusion and exclusion)
+ Review battery status and charging events
+ Perform remote alcohol testing

DNA leverages the power of Google Maps® to provide the most accurate display of a participant's location possible. Integrating Google Maps into the interactive mapping software allows DNA to provide a participant's current location (and location history) via Google's map view, satellite/aerial view, and street level view. Important features of DNA include:

+ Client Dashboard (page 42);
+ Real-Time Scheduling and Mapping (page 48);

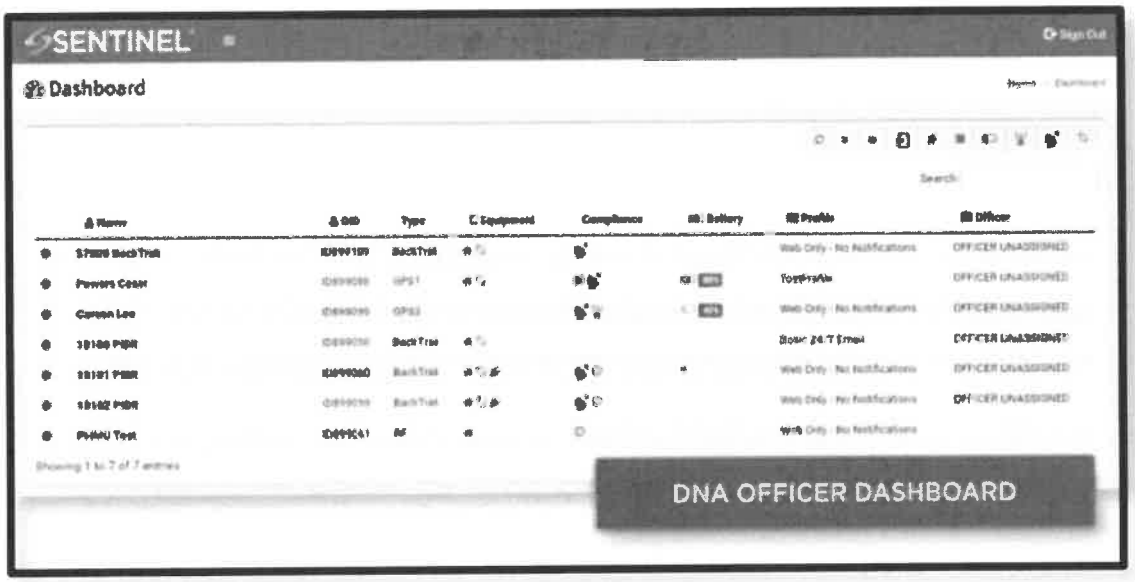
- Point Pattern Analysis (page 51); and
- Sentinel DNA Event Detection (Crime Scene Correlation) (page 53).

Sentinel's DNA, which is currently operating effectively in customer sites both domestically and internationally, offers advanced features and capabilities unavailable in other monitoring and tracking platforms:

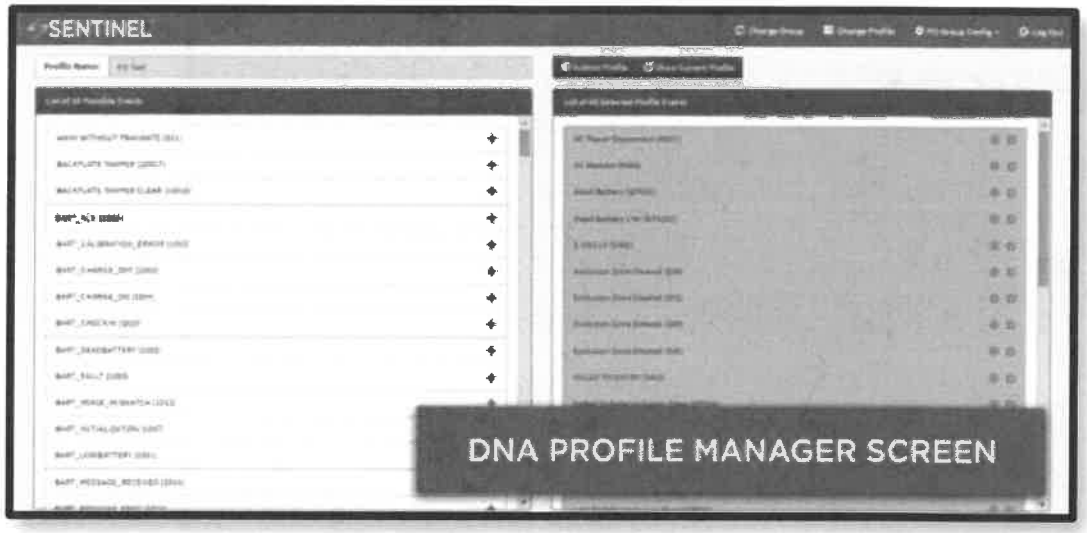
- Engineered, maintained and monitored exclusively by Sentinel;
- Fewer clicks with greater information access—DNA was specifically designed with officers in mind, where time is of the essence;
- Advanced automated screen resizing enables DNA to be accessed by desktops, laptops, tablets and by the majority of leading smart phone browsers without the need to download customer applications;
- Integration for all technologies (RF, GPS, Mobile Breath Alcohol, etc) into a single web-based platform;
- Advanced Dashboard for event management and alert processing;
- Google Maps for GPS providing enhancements such as "Street View";
- Automated Group Tracking Analytics of GPS Participants heightens officer attentions to comingling of GPS participants/locations;
- Point Pattern Analysis (PPA)/ Analytics provides automated detection/tracking of variances in participant movement patterns providing both graphical and mapping views to officers;
- Advanced Inventory Control Module enabling officers to track equipment in all capacities: in-use, in local inventory and in transit. This advanced module will also enable users to request/process/track/manage RMA's online via DNA;
- Advanced and extensive Report Library, and;
- Text Capability to the Home Monitoring Unit: Advanced capabilities to send DNA/web-to-PHMU/display customized alphanumeric text messages that prompt RF participants upon entering range of the PHMU and also record the participant's acknowledgement of receipt as web-based events within the participant's web-based activity.

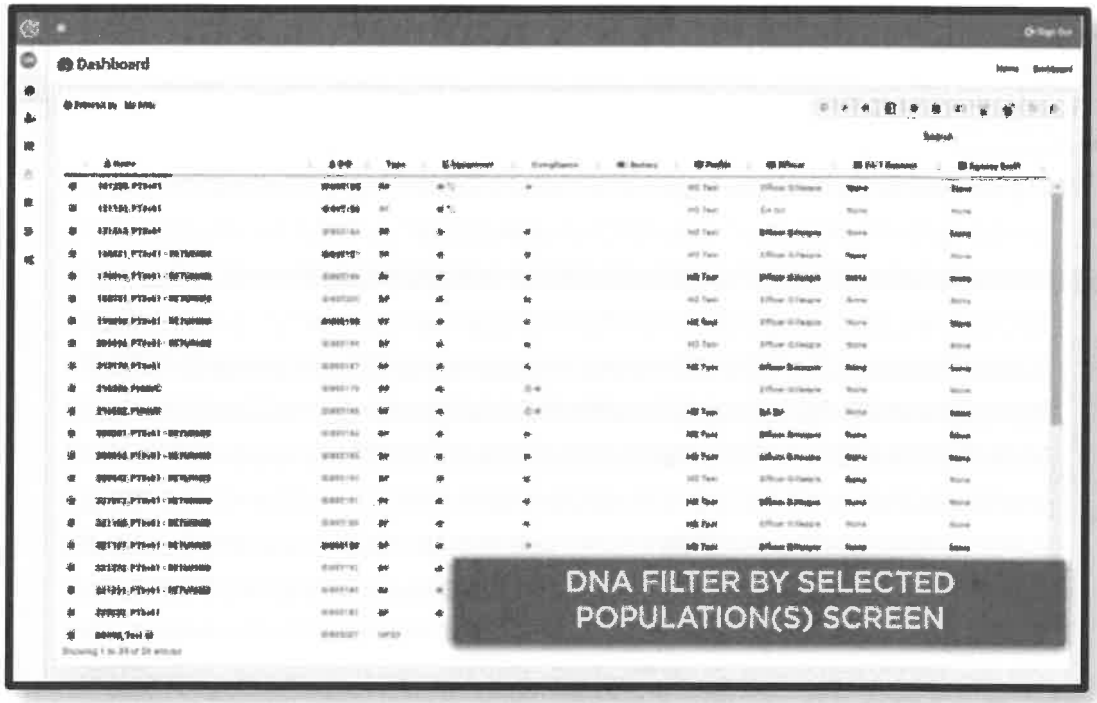
3.10.1 Client Dashboard

DNA utilizes a **Client Dashboard** that provides officers and case managers with the flexibility to view all or selected subsets of their entire caseload in real-time. Using straightforward alert icons, the client dashboard provides an easy to read at-a-glance interface that allows users to quickly see the status of participants. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events including *last known location* (via mapping), *current equipment status*, and *current battery status* including *recent battery events*, *zones*, and *schedules*.

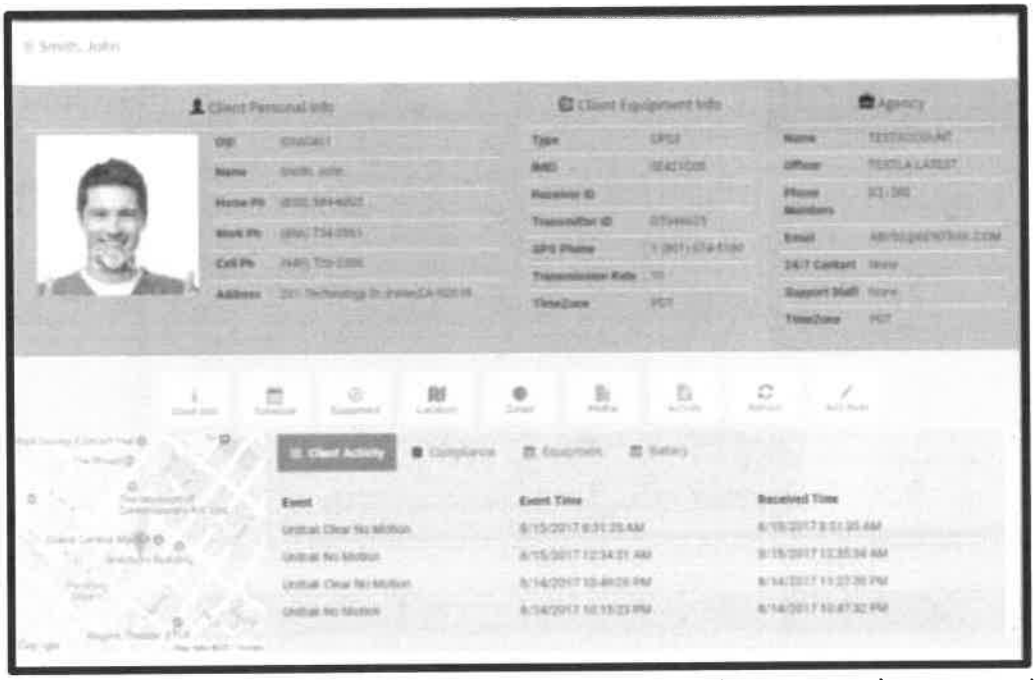


In addition, profiles, protocols, groups, and staff or agency contact designations can be used to further refine, sort, and filter populations. A complete local search option—as well as sorting and filtering options (shown below)—make it easy to refine the dashboard display to specific populations or participants with specific statuses.

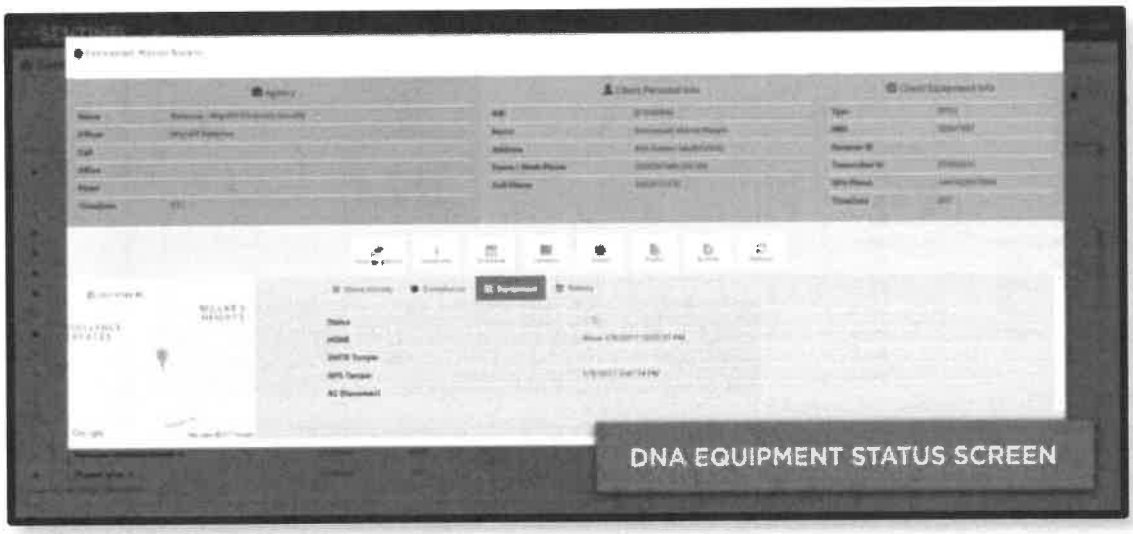




By clicking any of the fields on the Dashboard, an officer can easily access current and historical data for the client and the assigned equipment as shown in the screen images below. The Agency, Client Personal Info, and Client Equipment Info boxes at the top of the screen are static and provided at the top of all pop-up menus. Below we have provided an example of the **Client Activity** and **Equipment Status** screens.

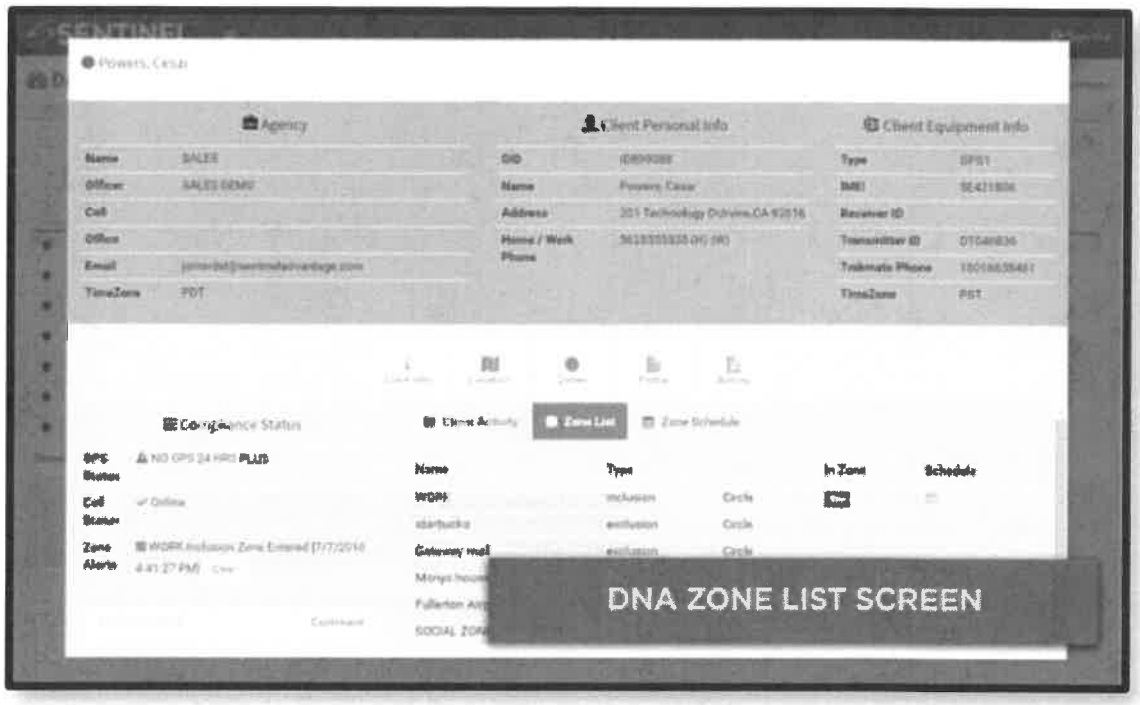


From the **Client Activity** screen above, the officer can access the participant's events to view additional data, see a quick snapshot of the participant's current location, access the participant's historical location data, view/create/edit/delete individual zones and review the protocols assigned to the participant.



As illustrated in the **Equipment Status** screen image above, the client's current location is shown on the map to the left along with the current status of the device including any tampers along with the date and time of occurrence.

As shown in the **Zone List** screen image below, an officer can see the client's current status along with their zones. The officer can also access the client's schedule allowing both zones and schedules to be easily updated at the same time.

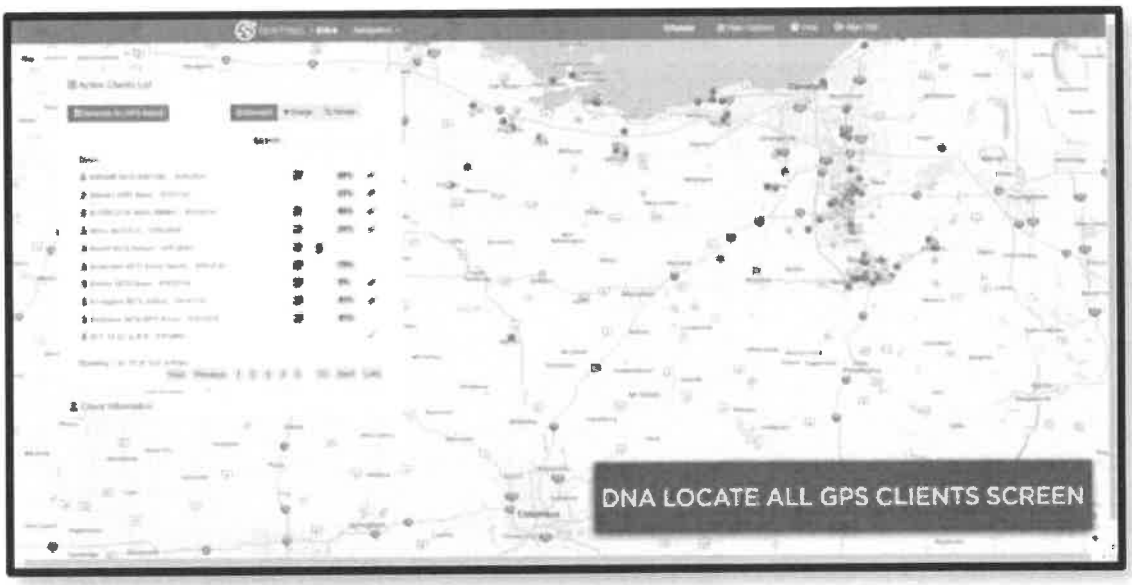


—IMPORTANT SENTINEL ADVANTAGE—

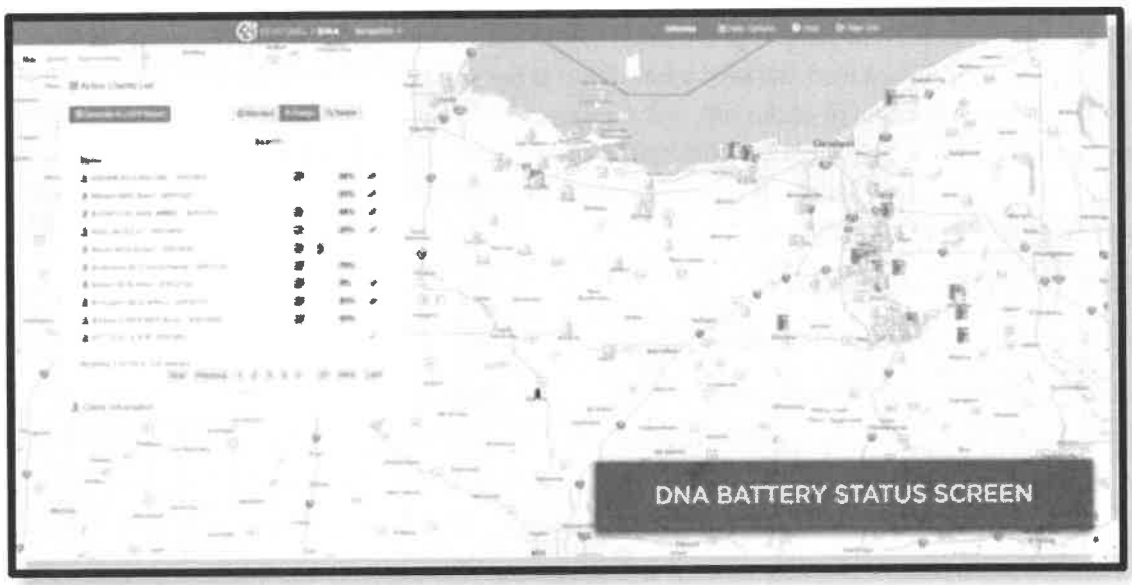
As an added service feature, DNA allows for use of *zone templates* that create pre-set zone placements for designated offenders. To simplify the creation and use of zones, DNA places an icon (depicted below) in every zone (individual client zone or group zone) to indicate the type of zone shown on a map. When an officer hovers over a zone icon, detailed information about this zone is displayed (e.g., name of the zone, the zone type [inclusion or exclusion], and zone size). This allows Sentinel and agency personnel to access meaningful location information while reviewing participant activity without move away from the monitoring screen. Inclusion Zones will be represented in the list by GREEN icons. Exclusion Zones will be represented in the list by RED icons.

CIRCLE Group zone = **BELL ICON**	
POLYGON Group zone = **SHIELD ICON**	
CIRCLE Individual Zone = **FLAG ICON**	
POLYGON Individual Zone = **UMBRELLA ICON**	

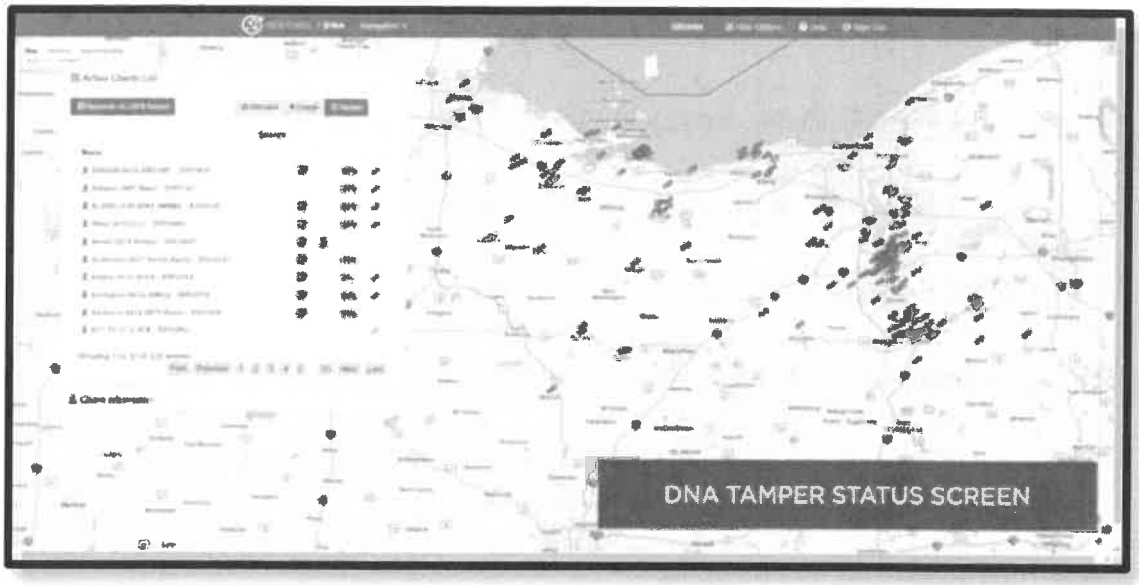
The DNA Mapping Software also gives officers access to locate their entire caseload by selecting ***Locate All GPS Clients*** from the Navigation Menu located at the top of the mapping. In this view shown below, the officer has the ability to see the battery status of the device as well as the current tamper status and whether the offender is at their residence/inside their home inclusion zone or is away.



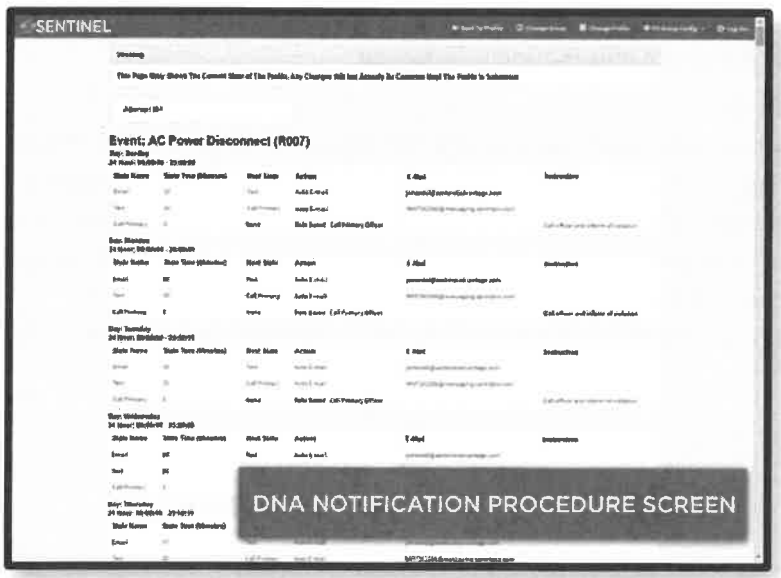
As illustrated below, DNA also gives officers the ability to view the battery status of every device assigned to their entire caseload from a single screen. DNA not only provides pop-up style notification windows to display case load details, the software also provides visual indicators for each participant on a map to the right of the case load window.



DNA provides the same detail regarding the tamper status of all devices assigned to an officer's entire caseload. As illustrated below, visual indicators help officers to quickly locate and identify potential issues and/or violations in their caseload.



DNA is equipped with the ability to create custom notification profiles. Each notification profile is a set of protocols on how to handle events and violations. Violations can be prioritized by type, by officer, and by participant to alert immediately or hold for a grace period. Additionally, notification procedures can also be customized by violation type, by participant, by risk or priority level, or by officer. The DNA profile manager also allows for automated or manual escalation and sequencing, as well as differentiating protocol changes within a single alert by day and time.



For added efficiency and convenience for officers, DNA provides the following enhanced features:

+ Users may choose to view "stacked" points on the map;
+ Users may run and export Points and Stops Reports from the participant location history;
+ Users may view all GPS Reports (Point or Stops) that have been generated from the View GPS Reports page;
+ Participant Information may be viewed in the View All GPS Clients or the participant View History page;
+ Address and time/date for each point is centrally displayed during point animation / VCR style playback;
+ Users may choose to view Group zones or Individual Zones on the map when viewing participant location history;
+ Zone icons have been added to help identify zone types. The name and size of the zone are displayed beneath the icon on the map;
+ Template and Individual Zones may be viewed from the View Client Zones page, and;
+ Participant location history defaults to the previous 24 hours.

3.10.2 Real-Time Scheduling and Mapping

Authorized personnel use our DNA Software Platform to enroll new participants and to see the latest activity and violation information. DNA allows users to view and modify all participant curfew schedules, alcohol schedules, battery charging schedules, and zone schedules as well as view and print monitoring activity reports for all participants. All features in DNA are available in real-time, any time, and anywhere via a completely web-based system.

DNA displays participant location information with specific date and time for each location. This chronological display is provided on screen as well as in printed report format. Users have the capability to select the exact method that data and event information is displayed.

—IMPORTANT SENTINEL ADVANTAGE—
As an added service feature, DNA allows authorized users to view the actual movements of the offender who has been assigned a GPS tracking unit, including the time of those movements, in a visual map and in report format. By clicking *Update Points* after selecting a date and time range, the user can *play* a participant's movements. The system will show the address of the tracking point when the user hovers over the tracking point with the mouse pointer. Users can view a participant's location (address, latitude, and longitude), time of location, and the rate of travel (speed) on the GPS Client History screen shown below.

During program enrollments, staff enter daily curfew schedules, alcohol testing schedules, battery charging schedules (if required by the program), and/or inclusion and exclusion zones for each offender in DNA. Each exit from, and entry to, the residence or zone (inclusion or exclusion) is reported by the GPS unit, and the DNA automatically compares the activity's location with the set zones. All battery alert and alcohol scheduling events (tests, missed, etc.) are reported by the individual units. Any discrepancies of the event time or location with the permitted time or location will generate a violation that is processed by DNA. This activity verification is continuously performed by DNA, which thereby ensures the monitoring of the offender population at all times.

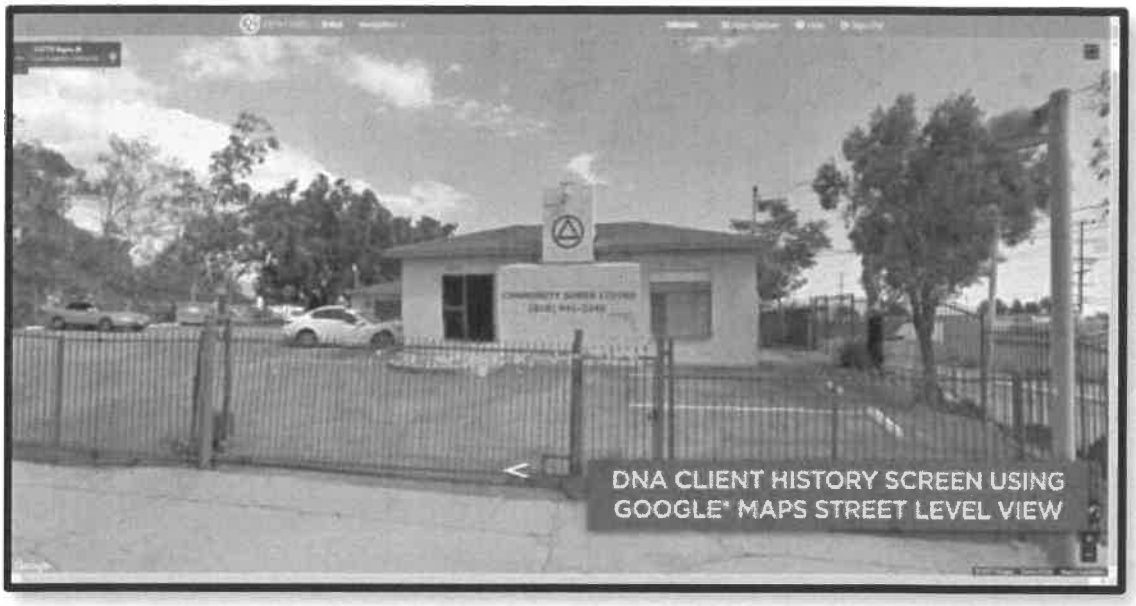
Additionally, users are able to create, edit, and delete exclusion and inclusion zones for participants being tracked via the GPS tracking device. These zones are used to control a participant's movements throughout the community. DNA allows for an almost unlimited amount of exclusion and inclusion zones per participant. For participants with challenging zones, DNA is also configured to support construction of polygon-shaped or *non-traditional zones*. These polygon zones can be used to customize the zone to whatever size or shape is desired by the officer to restrict the movement of the individual program participants.

Below are examples of a standard shaped inclusion zone (in GREEN) and a non-traditional polygon shaped exclusion zone (in RED). As shown in the images below, DNA visually differentiates zones with color-coding (Inclusion Zones = GREEN; Exclusion Zones = RED). As an added benefit, DNA allows for the creation of group zones that can be used across a specific population of participants. This allows agency personnel to designate certain sites across an entire region as restriction zones for an entire population. For example, DNA can establish pre-determined exclusion zones around schools, playgrounds or related areas for a given sex offender population to keep that entire population away from these zones. This removes the need to repeatedly re-create the same zones for all the individuals identified in a specific population. This type of group zone set-up can be used for sex offenders and other high-risk participant populations.

—IMPORTANT SENTINEL ADVANTAGE—

Google Maps® provides automatic updates to the DNA mapping software providing the latest in maps and upgrades at all times. Sentinel does not maintain maps within the software, unlike some vendors who must download regular updates to their mapping software which is a very time-consuming process. DNA tracks its own points and overlays the points on the most recent Google Map available from Google at the time of the tracking.

DNA uses Google Maps to provide authorized users with three (3) levels of mapping options: satellite images, street maps and hybrid maps (satellite imagery overlaid with street maps). These interactive maps contain easily recognizable images at the global level, state level and down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking maps. With the click of the mouse button, DNA allows authorized users to "drill down" from a high-level view of a defendant's location down to his/her tracking movements at a specific location.

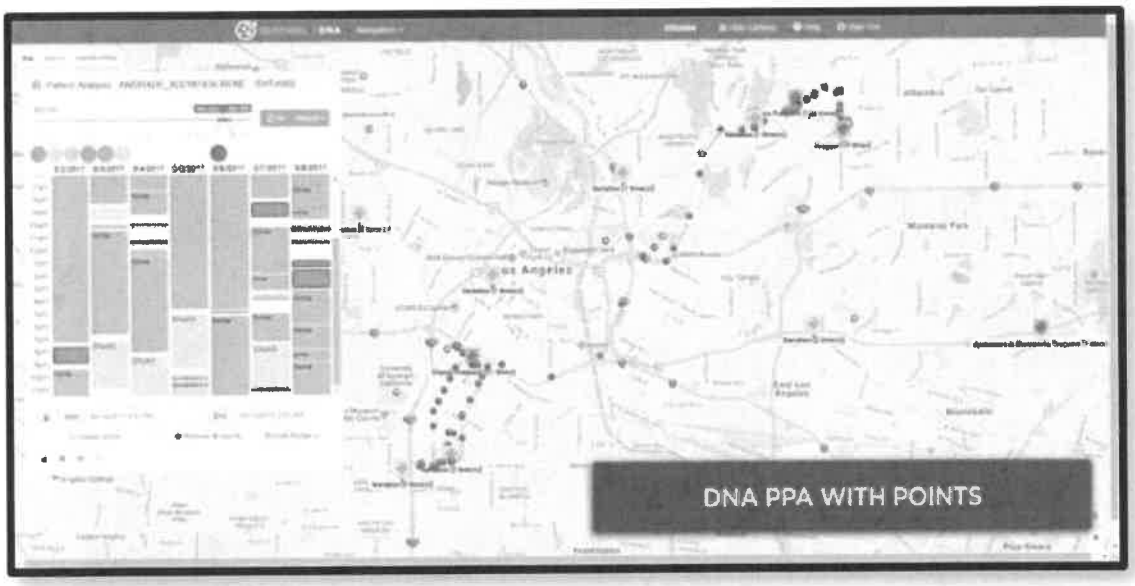


3.10.3 Point Pattern Analysis

In order to provide an agency with the most opportunities possible to create a positive outcome for the participant, DNA includes Point Pattern Analysis (PPA) capabilities. This proprietary enhancement feature allows users to comprehensive analysis of a given participant's daily routine.

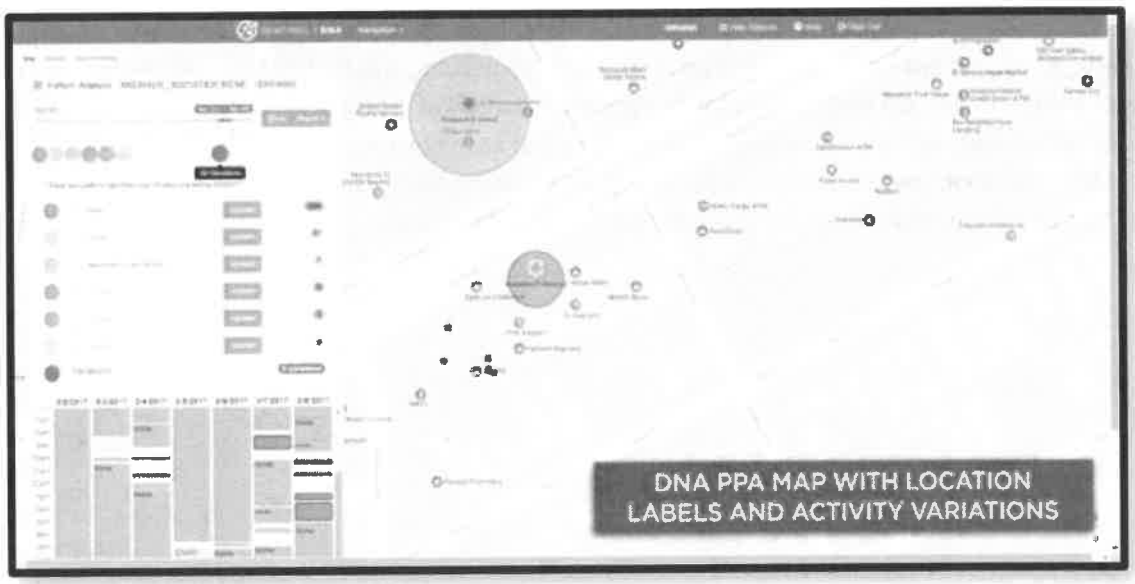
Using our GPS point capability, our software system is able to accurately track and display the participant's whereabouts 24/7. Although this is provided as part of the standard GPS tracking service, the advancement of this PPA feature is that it will display, in detailed chart format, the periods of time when an offender was at a certain location. The software then is able to track which locations the participant frequented and the quantity/duration of visits. This allows for easy determination of regular routine stops by the offender compared to variations that may be restricted locations.

Point Pattern Analysis analyzes locations frequented by each individual participant for enrolled in a program. Locations where a participant spends significant periods of time are identified and labeled as *known locations* and are depicted as such on DNA maps. For ease of review, the corresponding times spent at these locations are depicted on a bar graph (see below). All known locations are identified with a unique color system, while locations that are new for the offender are color coded in RED.



As an example, on the map display depicted above, a user can click on the locations and the position will be displayed on a Google map with all designated key identifiers (e.g., street names, locations of interest, civic structures, etc.) along with the ability to display the location in any of Google's multiple mapping views. DNA's flexibility allows for adjustment of parameters that dictate a new location compared to an established location.

To make the analysis of a participant's activity easier, DNA allows users to add labels to the locations that a participant visits as part of their daily, weekly or monthly routine (e.g., work, church, counselor's office, etc.) Using these labels allow for the quick identification of a location that is not associated with a participant's given routine. The screenshot below illustrates how users are able to create custom labels to better identify locations frequented by a participant.



3.10.4 Sentinel DNA Event Detection (Crime Scene Correlation)

Our Event Detection feature within DNA has a mapping component that correlates crime and incident report data collected from local law enforcement agency stakeholders and associates the crime data with the tracking data of participants.

Our Event Detection mapping feature will identify participants who were in the vicinity of a crime during a specific timeframe. Event Detection will simultaneously provide information for participants who are in the vicinity of the crime. Once the data has been entered, and the search has completed, the software will provide a Client List and place a flag on the map for each participant in the results list and represents the location of the participant that was closest to the search address during the time frame selected.

The search results are displayed under Client List. As illustrated in the screen image below, all the participants shown under Client List have registered at least one point within the search radius within the time frame selected.

4 SCOPE OF WORK

Sentinel understands the Lexington-Fayette Urban County Government Division of Community Corrections (Division) utilizes electronic monitoring as a population management alternative to institutionalization. Sentinel also understands the Division also utilizes electronic monitoring as an alternative sanction to the courts by implementing a home incarceration program engaged in protecting public safety and supervising those eligible offenders who pose a minimal risk to the community. As a leading provider of monitoring services and public safety solutions, Sentinel is able to provide advanced technology and services to help the Division meet their goals and objectives for the electronic home incarceration program. Sentinel is committed to providing the Division with state of the art technology and service and our goal is to draw on our past experience in order to provide the Division with a world-class program that will allow it to continue to perform its goals and objectives. We will provide the Division with access to state-of-the-art Radio Frequency Electronic Home and Curfew Monitoring, GPS Location-Based Monitoring Services, and Portable Breath Alcohol Testing that will assist the Division with reliably supervising offenders under established court orders for curfews, home confinement conditions, Stay Away Orders, and alcohol testing.

We believe our proposed solution will offer a cost-effective continuous electronic monitoring solution that provides proven, field tested equipment that is in use nationally and software that in many cases far exceeds the specifications as outlined in the RFP. Below, we have provided a point-by-point response to the Scope of Work.

C. MINIMUM VENDOR QUALIFICATIONS

1. The vendor must have at least three years recent experience in the electronic monitoring equipment industry.

Sentinel has been providing participant electronic monitoring and case management services for 25 years. Unlike other vendors, we focus 100% on the monitoring and tracking of participants. Sentinel is not a burglar alarm company or a non-corrections related firm. All of our services, products and technologies are specifically designed for corrections supervision. We provide 24 hour a day, seven (7) day a week, 365 days a year electronic monitoring and supervision services to more than 250 agencies across the United States. Our professional staff of nearly 250 employees is solely dedicated to providing services within the offender management market providing services to tens-of-thousands of individual participants on a daily basis through our monitoring center and a nationwide network of field offices.

2. The Vendor must have three years in the providing support services for the proposed field equipment, software and hardware for the on-site host computer.

All of Sentinel's services, products, and technologies are specifically designed for corrections supervision; we have been providing electronic monitoring and supervision services for 25 years. Our

professional staff of more than 200 employees is solely dedicated to providing services within the offender management market providing services to tens-of-thousands of individual participants on a daily basis through our monitoring center and a nationwide network of field offices.

3. The Vendor must have quality systems and standards in place that conform to the quality system standards of ISO 9001 for Design, Production, Installation, and Servicing of Electronic Monitoring Products and Electronic Monitoring Services.

a. The Vendor must provide a copy of this Certificate with its response.

Sentinel employs a Quality Management Program (ISO 9001:2008) that is designed to ensure specific policies and procedures are adhered regarding equipment manufacturing, software development, and monitoring services. The program requires our staff to report any customer complaint that is received. Further, the program dictates the steps that must be taken to investigate any concern by initiating a nonconformance report with the specific goal of identifying the root cause of an issue to ensure the effect of a permanent solution.

The Quality Management program is audited annually by an independent firm, American Systems Registrar, a provider of third-party system registration and accredited by the ANSI-ASQ National Accreditation Board. The audit consists of employee interviews to ensure that published policies and procedures are actually adhered by the staff. More importantly, the audit involves a thorough review of all nonconformance reports and their identified solution. On August 17, 2017, Sentinel obtained re-certification of our ISO 9001-2008 accreditation with "0" findings / non-conformities observed during the audit. The successful completion of Sentinel's audit demonstrates to our customer's our ability to:

+ Maintain our ISO 9001 certification;
+ Maintain and improve our level of quality;
+ Consistently deliver products and services to meet and exceed their needs; and
+ Improve conformity to quality requirements.

In addition, passing our 2017 ISO Surveillance Audit demonstrates the effectiveness of Sentinel's Quality Management System and confirms that our employees at every level are following Sentinel's Quality Management Plan with the goal of enhancing our customers' satisfaction.

Please see the **Supporting Documentation** (page 159) section of our proposal response for a copy of our ISO 9001:2008 certification.

4. The Vendor must provide documentation demonstrating the capability to provide remote 24/7/365 monitoring services for all equipment supplied under this RFP, including any redundancy developed as backups for the remote monitoring systems.

Sentinel's monitoring center has multiple disaster mitigation features, resides in an independently secured, climate-controlled facility with raised floors, has a fire suppression system, and written policies

and procedures for access. The monitoring center meets all applicable federal, state and local regulations regarding safety including building codes regarding earthquake resistance and hurricane resistance.

Sentinel's proposed solution maintains physical security compliance with all applicable Federal, State and local regulations. Also, the proposed Monitoring Application runs on a secure, highly reliable, redundant, and scalable carrier-grade infrastructure. The proposed datacenter environment was designed with redundancy in mind at every layer. The platform is deployed at multiple datacenters to provide geographical redundancy. The infrastructure operates with high-availability storage area networks and database clustering. The datacenters are supervised by live hardware and software engineers 24/7/365 to ensure the best possible uptime, and are supported with five (5) local internet loop providers with redundancy for every switch and component. This infrastructure and system capability has manifested itself in the achievement of 99.999% uptime, as measured, graded, and reported by one of the top three (3) carriers in the United States. Also, the proposed Data Centers are certified by the following:

+ ISO9001
+ SAS-70 Audited
+ HIPPA certified

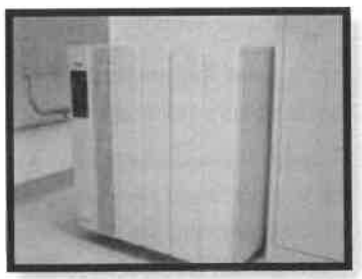
Data Center Security:

+ Four (4) physical layers of security
+ State-of-the-art access card system
+ Trained security personnel
+ Closed circuit television cameras (CCTV)
+ Biometric and Key Card secured facility
+ 24 hours a day, 7 days a week on-site staffing from dedicated security and storage engineers

The Data Center's electrical infrastructure consists of two (2) major components:

+ A Distribution System
  The distribution system has dedicated power sources that are provided by APS. The system is based on a redundant diverse distributed system consisting of Demarcation Power, Power Distribution Units (PDU), Uninterruptible Power Supplies (UPS) and a Utility Service Bus (USB). There are two (2) independent Utility Power Feeds on different sub-stations.

UNINTERRUPTIBLE POWER SUPPLY (UPS)



+ An Emergency Power Generation System
  The emergency power generation system consists of Automatic Transfer Switches (ATS), Emergency Service Bus (ESB), and redundant diesel generation. The primary system has a redundant backup system rated at 100% of the capacity of the primary system. In the event of a power failure, the

emergency diesel generators will provide power in less than 10 seconds and contain 1,000 hours of fuel for superior backup performance. Once started, the generator automatically ensures it is operating at sufficient capacity and then switches power from the grid to the generator. Data Center staff will conduct regular hourly inspections of the generator to ensure adequate fuel and proper operating parameters are maintained. The generator detects when the power grid resumes operation and within five (5) minutes restores power from the grid and shuts down the generator. This added redundancy virtually guarantees seamless and continuous power to the Data Center providing added confidence to the agency that public safety is ensured.

ON-SITE DIESEL GENERATOR

5. The Vendor must provide a Dunn and Bradstreet credit rating to determine financial stability.

Please see the **Supporting Documentation** (page 159) section of our proposal response for a copy of our Dun and Bradstreet credit rating.

D. GENERAL SYSTEM REQUIREMENTS

1. The base radio frequency system must be a continuous signaling, radio frequency-based transmitter and base station and require no active participation by the offender.

RF Patrol Electronic Monitoring Transmitter / Receiver

RF Patrol is designed to continuously determine whether or not a participant remains within a preset distance from the home monitoring unit located in their residence using a small, lightweight transmitter which is designed to be installed on the ankle of the participant. This equipment is capable of continuous signaling, receiving, storing and disseminating data generated by the system to the Sentinel monitoring center, all without any active participation by the participant.

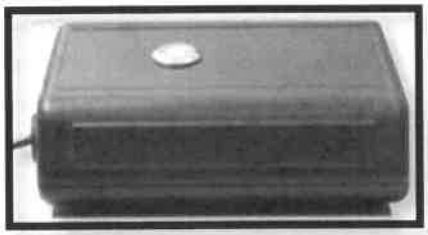
RF Patrol Suite

RF Patrol is specifically designed for house arrest monitoring and provides more reliable home supervision and intensive heightened notification including unauthorized absences, late returns, equipment malfunctions and tamper alerts.

OM400 GPS Tracking Device / Beacon

The OM400 RF Beacon is an *optional,* stationary, in-home monitoring device that can be paired with the OM400 GPS ankle bracelet to precisely verify home locations and extend valuable battery life. No active participation by the offender is required.

The OM400 RF Beacon uses radio frequency technology to provide the agency with an advanced solution to reliably monitor offenders in areas and environments where locations are problematic due to buildings or cellular coverage.



OM400™ RF BEACON

The OM400 RF Beacon offers the following features and benefits:

+ Accurately and reliably monitors curfews and reports all enters and leaves.
+ Monitors and reports A/C power disconnect, movement/relocation, and tampers.
+ Communicates over a proprietary encrypted signal to prevent false communication, jamming, and hacking.
+ Superior onboard memory in case of communication outage.
+ Internal backup battery lasts for up to 48 hours
+ Range of 150 feet

2. The monitoring equipment offered in the bid shall be fully supported by the original equipment manufacturer.

Sentinel confirms that all proposed equipment being offered is fully supported by the original equipment manufacturer.

3. The system shall use standard telephone lines and/or wireless cellular services to communicate between the individual transmitters/receivers and the monitoring center.

Sentinel's monitoring system receives event information from the proposed electronic monitoring equipment and accesses via cellular communication Sentinel's toll-free number to ensure there is no additional cost to the participant or agency.

4. The equipment and software provided must be the Vendor's most recent version released in the industry and upgraded as new versions become available at no cost to the Division.

Sentinel has proposed the most recent version of equipment and software released. As we strive to remain at the forefront of offender supervision technology, information for any equipment updates or upgrades can be provided to the Division as it becomes available.

5. The Vendor must supply all necessary tools and supplies to operate the system. Maintenance costs for the equipment shall be included as part of this proposal.

Sentinel will provide all necessary tools, straps, and other accessories for attaching, removing, and/or maintaining the proposed equipment at the Division's location at no charge. Maintenance costs for equipment will continue to be included at no cost to the Division.

6. The Vendor shall appoint a project manager who will also act as a contact and liaison for the Division.

Mr. Darin Simion will perform as the account manager/project manager during the program lifecycle. Mr. Simion will also be responsible for locally-based services in collaboration with agency staff as well as reviews of equipment use, participant activity and report interpretation. Mr. Simion will act as a contact and liaison for the Division as well as:

+ Conduct/assist with trainings and implementation
+ Be responsible for daily, weekly, and monthly reviews of inventory reports and any required KPI Reports
+ Be responsible for effective communication and customer service to customers

7. The project manager shall have, at a minimum, two years of work experience in electronic monitoring or the field of Community Corrections.

Mr. Simion has been a Sentinel Regional Account Manager since 2007 and has 14 years of experience in the electronic monitoring and community corrections industry. Mr. Simion will manage the day-to-day management oversight of the program as well as schedule training and webinar or refresher training sessions.

8. The project manager will schedule on-site visits with the department to review monitoring performance and to make any needed changes.

Mr. Simion will schedule on-site visits with the Division to review monitoring performance and to make any needed changes to the program.

9. The Vendor will provide the ability to register offenders into one or more of the various components via a Web-based interface.

Our monitoring system will be available to authorized Division users (username and password protected) at all times in real-time via any internet-enabled computer or device. Division staff will have

access to register, review and print offender information and/or activity and monitoring reports as needed.

10. The Vendor will provide qualified personnel in the event that expert testimony on functional aspects of the system and equipment is needed in Court for cases involving violations at no cost to the Division.

Sentinel understands the required testimony obligations, and we are fully prepared to provide qualified personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports while under oath in a court of law. Should the need occur for testimony in court upon request of the Division and/or in response to a subpoena, we will provide expert court testimony, either in person or written, through witnesses qualified to defend the integrity of Sentinel systems and services at no cost to the Division. Sentinel, with 25 years proven experience, has maintained integrity and credibility with numerous courts throughout the country on behalf of the agencies we serve. We will be able to submit the monitoring documentation as supporting evidence when describing the program participant's activities while monitoring.

11. The Vendor must be ready to proceed with provision and operation of the equipment within thirty (30) days after receiving a notice to proceed.

Sentinel stands ready to provide and operate the equipment and monitoring system within 30 days after receiving a notice to proceed.

12. Vendor must supply up to six replacement straps if the straps are reusable. This will cover straps that are damaged by the offender, at no cost to the Division.

We will supply up to six (6) replacement straps for the OM400 units at no cost to the Division. Sentinel's Account Manager will monitor the quantity of available spares to ensure that quantities meet the programmatic requirements.

E. GPS SYSTEM SPECIFICATIONS

1. The Vendor may have a unit that fulfils both the GPS and RFID portion of this RFP. The Division prefers a single piece GPS unit for higher risk offenders and the ability to monitor lower risk offenders with a 2 piece unit.

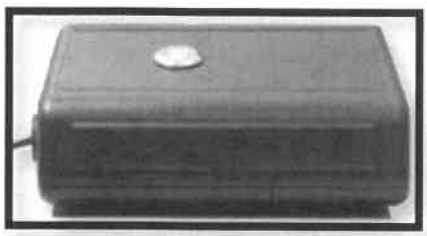
Sentinel is pleased to offer the Division the use of the OM400 One-Piece GPS Tracking and Location Based Monitoring Solution capable of monitoring and tracking inmate's movement reliably while ensuring compliance with established schedule.

The OM400 one-piece GPS device will track, locate, and verify an participant's locations while under the supervision of the Division, including reporting entries and exits from specified zones, equipment malfunctions. Sentinel operates a secure Monitoring Center 24 hours per day / 7 days per week / 365 days per year that can be contacted by agency personnel anytime.

The OM400 RF Beacon is an *optional,* stationary, in-home monitoring device that can be paired with the OM400 GPS ankle bracelet to precisely verify home locations and extend valuable battery life. The OM400 RF Beacon uses radio frequency technology to provide the agency with an advanced solution to reliably monitor offenders in areas and environments where locations are problematic due to buildings or cellular coverage.

The OM400 RF Beacon offers the following features and benefits:

+ Accurately and reliably monitors curfews and reports all enters and leaves.
+ Monitors and reports A/C power disconnect, movement/relocation, and tampers.
+ Communicates over a proprietary encrypted signal to prevent false communication, jamming, and hacking.
+ Superior onboard memory in case of communication outage.
+ Internal backup battery lasts for up to 48 hours
+ Range of 150 feet



OM400™ RF BEACON

2. The vendor shall provide the option to the division to issue a cell phone to the individual participant by which they can be contacted by the Division or receive alert notifications.

Sentinel understands the importance of having the ability to verbally communicate with program participants at all times while on the program. As such we will provide the Division with ten (10) voice- and text-enabled cell phones at no cost that can be issued to program participants as deemed appropriate by Division personnel. Additional cell phones can be made available at a minimal cost as provided within the Equipment Lease Cost section.

3. The Vendor should be able to demonstrate that its GPS system is capable of tracking individuals by use of its system 24 hours a day.

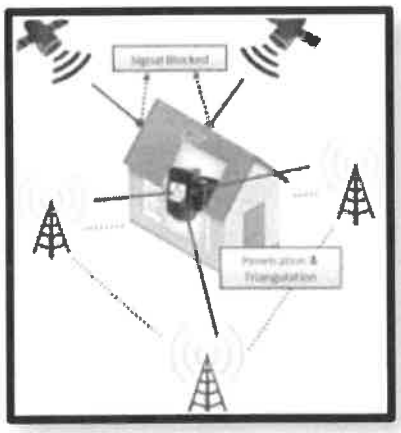
The OM400 GPS tracking solution is specifically designed for the criminal justice industry and provides reliable, continuous 24 hour a day, seven (7) day a week, 365 day a year offender tracking via GPS

technology. The OM400 GPS device being offered herein continues to be the one-piece GPS product of choice by those agencies who have conducted field testing of multiple GPS devices prior to making an award. The OM400 GPS device is both the receiver of location information and the transmitter of status and location information and is supported by an innovative, user-friendly web-based information exchange.

4. The system must have a secondary system to track offenders in the event a GPS signal is not available. (Example: Cellular Triangulation) The system must be able to determine the offender's location to within fifty (50) feet.

The location-based monitoring equipment offered by Sentinel is unique from other GPS offender tracking devices in that Sentinel's proposed device uses both GPS and Advanced Forward Link Trilateration (AFLT) technologies to track offenders' locations. This dual-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking.

The OM400 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM400's unique design combines multiple layers of location technologies including AFLT (Advanced Forward Link Trilateration), GPS, and Assisted GPS (A-GPS). Such technology allows for reliable location information to be processed anywhere and compensate for poor GPS availability in GPS-impaired environments. The combination on these advanced location technologies allows for the quickest acquisition time (typically within 60 seconds, so long as there a cellular signal detected) without an office being required to go outside to acquire a GPS signal when enrolling and installing a device.



The OM400 acquires GPS utilizing a system of satellites signals and, in the event the OM400 can only find a few GPS satellite signals due to partial blockage or location, it willautomatically shift to A-GPS. With A-GPS, the OM400 uses the available GPS signals in combination with cellular network data. In the instance of impaired GPS, or no GPS signal, the OM400 activates Advanced Forward Link Trilateration (AFLT). The AFLT triangulates utilizing ambient longitude and latitude data broadcast by the cellular environment. This is a unique capability and is possible with devices communicating via a CDMA cellular network.

The OM400 communicates via the **Verizon or Sprint** networks, both CDMA-based. Designed to track and allow communication with the offender 24/7, the OM400 locates indoors and out. As with typical GPS, interference is a reality and in any case, there are two (2) formats of signal that can be impacted; GPS and cellular signal. Such obstacles are geographic in nature (poor GPS location), signal disruptors (scramblers, shielding, tracing, and duplication), cellular turndown (termination of many 2G GSM networks as announced by AT&T), and locations with poor cellular reception. Taking these obstacles in

mind, the OM400 technology is centered on reliably offering two (2) cellular networks - Verizon and Sprint - to heighten cellular options and provide reliable location data in GPS-impaired locations. The OM400 uses the CDMA wireless digital cellular standard to transmit and communicate data directly to the monitoring system via two (2) of the largest cellular networks in the world. The OM400 device uses encrypted communications that prevents tracing and duplication. Additionally, the OM400, through its CDMA communication capabilities, is not subject to the eminent, and in some cases immediate, "turndown of service" that has been announced by major GSM networks like AT&T. Therefore, there is no threat of interruption of service.

All GPS manufacturers utilize the same government satellites; therefore, all GPS leading systems are comparable in accuracy terms as the accuracy is directly related to the number of satellites that are being received by the GPS receiver; the more satellites the more accurate the positioning fix. The accuracy could roughly be broken out as shown in the following table:

NUMBER OF SATELLITES	DEGREE OF ACCURACY
1 - 2 satellites	No fix can be established
3 - 4 satellites	30-meter accuracy
4 - 6 satellites	10 - 30-meter accuracy
7 - 9 satellites	3 - 10-meter accuracy
10 or more	Better than 3-meter accuracy

GPS accuracy can vary with any GPS manufacturer based on the satellite reception at any given point therefore it is important for officer's to be able to promptly determine the accuracy of any tracking point in order to determine the basis for compliance and/or potential violation. The AFLT may enable tracking in such impaired locations with a point accuracy of better than 30 feet.

---

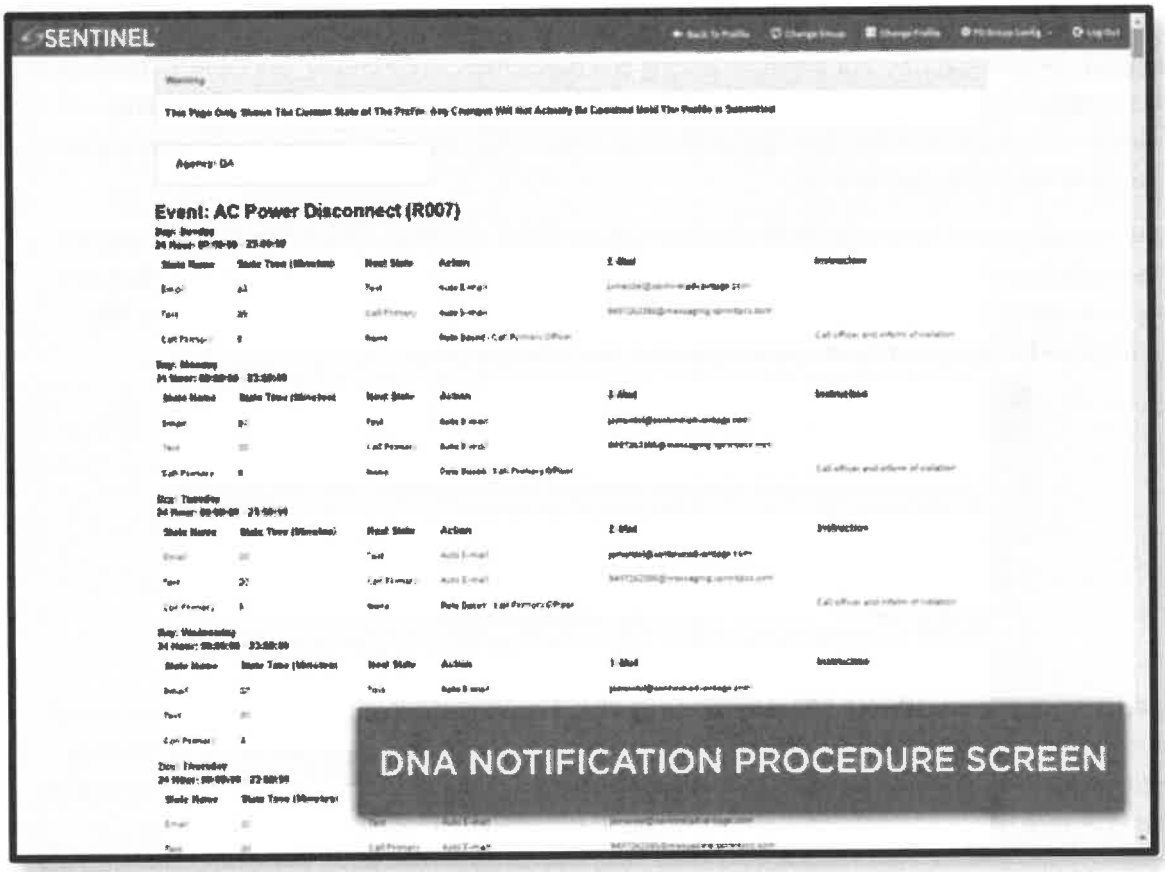
5. The system must be able to provide the Division with automatic alerts on Failure to Track, Violations of Exclusion and Inclusion Zones, and Transmitter and Strap Tampers. It should also be able to generate on demand reports such as offender history and background.

Sentinel's monitoring system will be able to provide the Division with automatic alerts on Failure to Track, Violations of Exclusion and Inclusion Zones, and Transmitter and Strap Tampers. Sentinel's monitoring system is also capable of generating on-demand reports such as offender history and background.

Through our DNA monitoring platform, Sentinel provides alert notifications to its customers for a wide array of violations and events. The DNA system supports different methods of alerting proper personnel of violations or events including an immediate email message, a pager message, or a text message.

DNA is equipped with the ability to create custom notification profiles. Each notification profile is a set of protocols on how to handle events and violations. *Violations can be prioritized by type, by officer, and by participant to alert immediately or hold for a grace period.* Additionally, notification procedures can also be customized by violation type, by participant, by risk or priority level, or by officer. The DNA

profile manager also allows for automated or manual escalation and sequencing, as well as differentiating protocol changes within a single alert by day and time.



Please note: As the Sentinel monitoring software is an in-house concept and design, the system is regularly upgraded to meet changing program needs and the changing needs of Sentinel's program partners. Sentinel is not reliant on an outside vendor for new editions or support. Sentinel will work with each agency to enable the features that the agency wants and disable those that it does not want.

6. The system must be capable of sending immediate violation notifications via ~~fax~~, telephone (landline), cell phone, email and pager or to a designated contact point or person(s). The system should also be capable of having various security levels or violation notifications set by the Division for offenders. **[Struck per Addendum # 1]**

Sentinel's monitoring system will provide direct notification as required 24 hours a day, seven (7) days a week regarding the events and violations of participants enrolled in the Division's program. Additionally, our monitoring center is staffed 24 hours a day, seven (7) days a week with live operators who respond per program procedures to participant data as well as provide technical support to agency staff.

Our web-based monitoring system, which receives all data generated by the field equipment, allows for authorized personnel to determine alarm and notification protocols. Depending on the Division's notification requirements, Sentinel can provide notifications to responsible parties according to notification type, participant type and agency-specific rules. Sentinel offers notification through various methods based on levels of urgency. The methods Sentinel uses for notification include the following:

+ Cellular and landline phone
+ Alpha Pagers
+ Email notifications
+ Direct phone calls to designated agency staff

Our monitoring system allows for authorized personnel to determine alarm and notification protocols. Prior to deployment, Sentinel's operations team can meet with LFUCG and Division personnel to establish group level alarm and notification protocols. Once these groups, such as "high risk", are established, the Division can place individuals within the specific group and receive alarms and notifications as dictated by the pre-determined protocols for that group. All event notifications can be sent to various parties, including case workers, field agents, local law enforcement personnel, and third-party systems. Depending on the notification requirements, Sentinel can provide notifications to responsible parties according to notification type, participant type and agency-specific rules. Sentinel offers notification through various methods based on levels of urgency.

The notifications capability of the monitoring software includes but is not limited to:

+ Violations of inclusion and exclusion zones
+ Unauthorized absences from the residence
+ Authorized exits and enters from the residence
+ Failure to return to residence from a scheduled absence
+ Late arrivals, early departures from residence
+ Tampering with equipment
+ Loss of electrical power or telephone service
+ Restoration of electrical power or telephone service
+ Missed calls from receiver/dialer

+ Low Battery alerts from any component

7. The Vendor must supply the Division with a web based offender tracking site available 24 hours per day, seven days a week to review location history, information, offender status, and enter/remove offenders from the program. This site should also be compatible with the radio frequency system.

DNA is our state-of-the-art web-based monitoring and tracking software platform that will be available to authorized Division users (username and password protected) at all times in real-time. Designed in-house by Sentinel software engineers, DNA can be customized to include all required reports, notification procedures and escalation alert sequencing. DNA will allow the RF Patrol electronic monitoring, OM400 GPS tracking, and BA/RT breath alcohol monitoring technologies proposed herein to communicate on a single web accessible platform. Moreover, this powerful and easy to use platform will provide the Division with customizable features and benefits not available from other monitoring software solutions. In addition to reports and notification procedures, Division staff will have access to review location history, information, offender status, and enter/remove as needed. Authorized users will also be able to access the GPS tracking data via the internet-enabled monitoring system.

8. The system must provide active (1 minute GPS fix / 1 Hour transmit / 15 impaired location) and passive (1 minute GPS fix / 3 hour transmit / 30 minute impaired location) tracking capabilities without the changing of equipment and/or software. Equipment must have ability to transition to active status when in violation.

The OM400 unit is both the transmitter and receiver of information in one (1) unit and is equipped with on-board processing capabilities. The unit will track at one (1) point per minute and store several days of tracking information in the on-board memory, regardless of the mode of operation, should the unit be unable to communicate with the monitoring application. The OM400 is also able to store zones on board the device in order to provide immediate notifications on zone alerts. Through the supporting monitoring software application, our proposed solution provides the flexibility needed for controlling the level of supervision each participant receives to meet individual monitoring demands. This level is defined by the type of monitoring assigned in the participant's profile. The profile not only defines the monitoring intensity, but also allows our staff to change the level as directed by the referring agency, based on a participant's current monitoring status. Sentinel's DNA platform provides the flexibility to include multiple tracking capabilities with the ability to transmit data at time intervals determined by the Division. Profiles available include the ability to track on a minute-by-minute basis if desired. These profiles will be determined by the Division and made available on a participant by participant basis through the profile selection process. The most common profiles are identified below but may be customized to meet program requirements.

RISK PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point either in 60 second increments and transmits data every 10 minutes and includes an	Riskiest participants requiring a very high

	Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	level of supervision
Hybrid Monitoring	Acquires a GPS point every 60 seconds and transmits data every 30 minutes and includes an Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every 60 seconds and transmits data every 60 minutes and includes an Impaired Locate every 60 minutes. Tampers and zone violations are immediately transmitted.	Less risky participants requiring only strong supervision

The monitoring application allows our staff to set up advanced warning parameters in order to create buffer zones around exclusion zones to alert individuals of an upcoming potential violation of the zone.

Buffer zones provide an extra layer of security around exclusion zone borders, and enhance notifications and rapid response to exclusion zone violations. A buffer zone is an extended area surrounding an exclusion zone. Once the buffer zone is breached, a Buffer Zone Alert is generated and the device increases its GPS acquisition and cellular transmission rate to real-time tracking: 1 minute by 1 minute. This puts monitoring personnel on alert and allows for early intervention before the exclusion zone is breached. Tracking will continue in real-time to provide the fastest possible notification on proximity to the exclusion zone until the participant has cleared the area.

Mobile Exclusion Zones (MEZ) allow agencies to ensure that a participant on monitoring does not come near another specific individual anywhere they may be. Taking monitoring beyond stationary zones, the MEZ program monitors the activity of two GPS devices to determine their proximity from one another in the real world. Often used for victim protection and in domestic violence cases, the victim carries a device while the participant wears one. If the two devices come within a specified distance of each other, notifications are generated and law enforcement may be contacted. The victim may also be notified, giving her necessary information to help her find safety.

I. GPS TRACKING UNIT SPECIFICATION

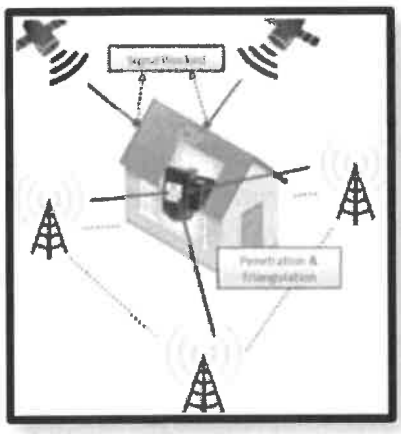
1. Vendor may offer GPS tracking units, which can be tracked utilizing a smart phone. One (1) smart phone for alert notification, tracking, and contact with participants may be made available to the Division at no additional cost.

Sentinel is proposing the OM400 one-piece GPS device and our DNA monitoring platform for use in this program. Sentinel's DNA monitoring platform may be accessed by authorized users having a secure username and password through any internet-enabled device including smartphones, tablets, laptop computers, and desktop computers. We understand the importance of Division personnel having the ability to receive alert notifications and review tracking data while in the field and/or away from the office. We also understand the importance of having a means of communicating with the participants at all times. As such, Sentinel will provide one (1) smart phone for use by Division personnel at no additional cost.

2. The GPS tracking unit should be capable of monitoring an offender's movements at any time and in any location.

The OM400 GPS units are always active and communicate through cellular coverage; therefore the unit is capable of monitoring an offender's movements at any time and in any location.

The OM400 uses both GPS and Advanced Forward Link Trilateration (AFLT) technologies to track offenders' locations. This dual-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking.



The OM400 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM400's unique design combines multiple layers of location technologies including AFLT (Advanced Forward Link Trilateration), GPS, and Assisted GPS (A-GPS). Such technology allows for reliable location information to be processed anywhere and compensate for poor GPS availability in GPS-impaired environments. The combination on these advanced location technologies allows for the quickest acquisition time (typically within 60 seconds, so long as there a cellular signal detected) without an office being required to go outside to acquire a GPS signal when enrolling and installing a device.

The OM400 acquires GPS utilizing a system of satellites signals and, in the event the OM400 can only find a few GPS satellite signals due to partial blockage or location, it willautomatically shift to A-GPS. With A-GPS, the OM400 uses the available GPS signals in combination with cellular network data. In the instance of impaired GPS, or no GPS signal, the OM400 activates Advanced Forward Link Trilateration (AFLT). The AFLT triangulates utilizing ambient longitude and latitude data broadcast by the cellular environment. This is a unique capability and is possible with devices communicating via a CDMA cellular network.

The OM400 communicates via the **Verizon or Sprint** networks, both CDMA-based. Designed to track and allow communication with the offender 24/7, the OM400 locates indoors and out. As with typical GPS, interference is a reality and in any case, there are two (2) formats of signal that can be impacted; GPS and cellular signal. Such obstacles are geographic in nature (poor GPS location), signal disruptors (scramblers, shielding, tracing, and duplication), cellular turndown (termination of many 2G GSM networks as announced by AT&T), and locations with poor cellular reception. Taking these obstacles in mind, the OM400 technology is centered on reliably offering two (2) cellular networks - Verizon and Sprint - to heighten cellular options and provide reliable location data in GPS-impaired locations. The OM400 uses the CDMA wireless digital cellular standard to transmit and communicate data directly to the monitoring system via two (2) of the largest cellular networks in the world. The OM400 device uses encrypted communications that prevents tracing and duplication. Additionally, the OM400, through its CDMA communication capabilities, is not subject to the eminent, and in some cases immediate,

"turndown of service" that has been announced by major GSM networks like AT&T. Therefore, there is no threat of interruption of service.

Additionally authorized users will have access to our DNA monitoring software platform and will be able to "ping" the OM400 unit in order to determine the unit's current location. The OM400 device can be beeped through the monitoring software, and this feature can be activated to assist in locating the unit.

3. The GPS tracking unit device should be a one piece unit and fit on the offender's ankle and should be lightweight.

The OM400 is a discrete unit that is easily, securely and comfortably attached to the ankle of participants under normal slacks. The OM400 tracking device is a one-piece device that is FCC certified (FCC ID AB3-OM400) and is a small and light weight with the device's dimensions at approximately 3.5 x 2.4 x 1.6 inches and weighs 8.4 ounces.

4. The GPS tracking unit should have the ability to vary rates of GPS recording from 1 to 10 minutes. The capability should be configured in the individual clients setup information by the Division via the Web interface and provide for downloading new updates over the phone line.

The OM400 unit is both the transmitter and receiver of information in one (1) unit and is equipped with on-board processing capabilities. Through the Sentinel DNA web-based monitoring system, authorized Division users will be able to configure the individual client's setup information. The OM400 provides variable rates of GPS tracking and reports the information based on the tracking level/rate plan selected during participant enrollment or record editing. Division staff can also provide the information to Sentinel monitoring center operators over the phone for setup within the system when a computer or mobile device is not available to them. Any changes made to a participant's tracking level/rate plan are pushed to the OM400 unit via cellular communication.

The unit will track at varying rates, including from one (1) to ten (10) minutes, all of which are determined by the Division and available during participant enrollment as well as during client record editing. The most common rate utilized by programs throughout the country, one (1) point per minute, allows for the acquisition of a GPS location every 60 seconds. The OM400 can store several days of tracking information in the on-board memory, regardless of the mode of operation, should the unit be unable to communicate with the monitoring application. The OM400 is also able to store zones on board the device in order to provide immediate notifications on zone alerts. Through the supporting monitoring software application, our proposed solution provides the flexibility needed for controlling the level of supervision each participant receives to meet individual monitoring demands. This level is defined by the type of monitoring assigned in the participant's profile. The profile not only defines the monitoring intensity, but also allows our staff to change the level as directed by the referring agency, based on a participant's current monitoring status. Profiles available include the ability to track on a minute-by-minute basis if desired. The most common profiles are identified below but may be customized to meet program requirements.

RISK PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point either in 60 second increments and transmits data every 10 minutes and includes an Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every 60 seconds and transmits data every 30 minutes and includes an Impaired Locate every 15 minutes. Tampers and zone violations are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every 60 seconds and transmits data every 60 minutes and includes an Impaired Locate every 60 minutes. Tampers and zone violations are immediately transmitted.	Less risky participants requiring only strong supervision

5. The GPS tracking unit should be water resistant and shock resistant and able to withstand normal daily use.

The OM400 GPS tracking device is small, lightweight and does not inhibit participant activities. The OM400 device casings are hardened and waterproof in both salt water and fresh water. The units can withstand temperatures between -68° Fahrenheit and 140° Fahrenheit, and up to 500 MHz of random vibration of 1.25G rms. The OM400 will function under normal household, atmospheric and environmental conditions. The OM400 does not pose a safety hazard or unduly restrict the activities of the offender. It is also dishwasher safe, which is the easiest and safest way to sterilize the device.

6. The GPS tracking unit should be tamper resistant.

The OM400 GPS tracking device detects three (3) tamper types including 1) strap tamper, 2) device case tamper and 3) backplate tamper. Within seconds of a tamper attempt, the device will communicate and send a unique alert to the monitoring system web interface. The OM400 device will automatically communicate to the monitoring system software when a participant attempts to remove or tamper with the strap. The monitoring system then sends the alert to the appropriate agency defined personnel. The OM400 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit.

When properly installed, attempts to defeat, remove or tamper with the OM400 GPS tracking device will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The backplate fits precisely in place and any attempts to pry it open are easily noticeable.

The OM400 devices offer the most advanced tamper detection and reset methodology. The devices have been proven to be highly reliable and reduce the production of false tampers. The devices remain

in tamper until inspected and reset through the monitoring system software. The reduction in excessive tamper events that are a nuisance to officers reduces tamper events to only those that truly warrant investigation and necessitate oversight. If an officer is not near a computer, he or she may call the Sentinel monitoring center to clear any tamper event. Our DNA monitoring platform is available via any internet enabled device to allow officers to clear alerts or access participant activity when away from the office.

7. The GPS tracking unit shall provide Division staff with the tamper status of the transmitter and the battery status of the transmitter when a transmitter signal is detected.

The OM400 device will provide the tamper status and battery status of the unit in each communication with the monitoring system. Additionally, the OM400 will automatically and instantly communicate to the Sentinel DNA software when a participant attempts to remove or tamper with the strap or when the battery is low. The Sentinel DNA system then sends the alerts to the appropriate agency defined personnel.

The OM400 will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit.

When properly installed, attempts to defeat, remove or tamper with the OM400 will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The backplate fits precisely in place and any attempts to pry it open are easily noticeable.

Additionally, the unit will emit a low battery alert when the battery reaches a threshold of 35-40% of remaining battery power.

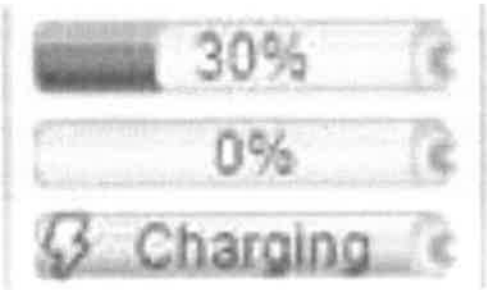
8. The battery in the GPS tracking unit should be durable and should be rechargeable. The Vendor should indicate whether the receiver battery is replaceable in the field or that it needs to be returned to the Vendor for replacement. The battery's daily charge should be sufficient to allow an offender to be gone from home for up to twenty-four (24) hours between charges.

The OM400 tracking device is designed for long-term use in the field; the unit is durable and easily rechargeable. The unit is sealed to ensure that is it water resistant and therefore is not equipped with a battery that can be replaced in the field; it must be returned to Sentinel's warehouse for replacement.

The unit has an intensive monitoring battery up-time of up to 72 hours depending upon the rate plan used by the agency and is rechargeable in 1.5 hours. Participants charge the unit through a standard 110V plug with a 15-foot cord easily connected directly to the front of the unit. The OM400 features a multi-colored LED light that will illuminate during battery charging.

OM SERIES LED LIGHTS

Additionally, the device reports the battery status each time it reports to the monitoring center. If the device's power is low, the monitoring center will generate a low battery alert. A low battery alert is generally generated when the device is at 20% or less of battery power. This alert will clear when battery power is restored above 85%. To mitigate low battery issues, agencies can incorporate a mandatory recharging schedule into the participant's daily schedule. If the device is not charging at the scheduled time, or if it is unplugged prior to the expiration of the charging schedule, the monitoring center can notify staff if required. The software also allows the agency to require the OM400 device to take specific action such as vibrating to alert the participant in the event of a low battery.



OM SERIES BATTERY STATUS

9. The GPS tracking unit should be capable of continuing to monitor the offender while it is being charged.

The OM400 will continue to monitor the offender while the unit is being charged.

10. The GPS tracking unit (or system) should be capable of establishing Exclusion Zones where a violation report will be generated when the offender moves into that zone. The system should also be able to establish Inclusion Zones where the offender is permitted to be and a violation report will be generated when they move outside of these zones.

Using Sentinel DNA, authorized personnel are able to create, edit and delete Exclusion and Inclusion zones for participants being tracked via the GPS one-piece unit. These zones are used to control a participant's movements throughout the community. Sentinel DNA allows for an almost unlimited amount of Exclusion and Inclusion zones per client. For participants with challenging zones, Sentinel DNA is also configured to support construction of polygon-shaped or non-traditional zones. Sentinel DNA visually differentiates zones with color-coding, as follows: Inclusion Zone = Green; Exclusion Zone = Red.

If a participant moves into or out of an Exclusion Zone or leaves an Inclusion Zone, the OM400 records the location of the participant and a violation notification is automatically sent to the applicable Division officer upon reporting this violation to the system. The Sentinel DNA system will also alert applicable Division officers when a participant enters or leaves a Buffer Zone.

11. The Zones shall be capable of being customized by Division staff via Web-based access.

Zones can be customized by Division staff via the web-based Sentinel DNA monitoring system. Authorized staff will have the ability to create inclusion zones that are geographic areas where an offender is scheduled to be, such as home or work; they will also have the ability to create exclusion zones, which are geographic areas where the offender is not permitted to visit such as a victim's home, schools, or areas outside the state or county border. In addition, the proposed monitoring software application provides the ability to configure zones in the shapes of circles, rectangles, and arbitrarily shaped polygons, as well as be able to have zones within zones.

Zones can be created as offender zones, if only one offender will need to use the zone, and company zones that can be created and stored within the system as a library of zones in the event there are multiple offenders who need to use the same zone. Some examples of company zones include schools, parks, and/or day care centers. Authorized staff will be able to create groups of company zones that can

be assigned or unassigned from the group and a schedule for the group zones can be created with a single entry.

—IMPORTANT SENTINEL ADVANTAGE—
Authorized staff will have the ability to upload circular and rectangular zones to the device in order to generate immediate notifications when a zone is crossed. This capability allows for near real-time alert notifications and processing. The agency will have the ability to designate to our staff which circular and/or rectangular zones they would like uploaded to the device to allow for those immediate notifications and processing by the monitoring center.

12. The GPS tracking unit should record if the offender moved into or out of an Exclusion Zone or leaves an Inclusion Zone and transfer the recorded data.

The OM400 device incorporates a cellular modem and communicates information to the monitoring center over the CDMA cellular network at programmed call in times as determined by the selected rate plan. If a participant moves into or out of an Exclusion Zone or leaves an Inclusion Zone, the OM400 records the location of the participant and a violation notification is automatically sent to the applicable Division officer upon reporting this violation to the system.

13. The GPS tracking unit (or system) will generate a report when the cellular and/or the GPS signal is lost and the system can no longer track the offender or communicate with the data storage unit.

The OM400 will record and report to the monitoring center when the cellular and/or GPS signal is lost. The Sentinel DNA system will automatically produce either a "Location Failure" or "Communications Failure" and notify the appropriate officer with the alert based on user defined notification protocols.

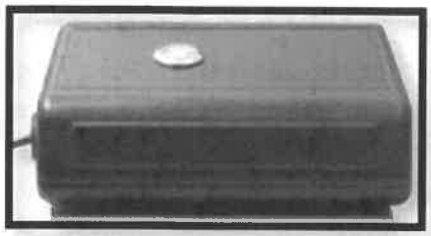
14. The GPS tracking unit will not be affected by the operation of other electronic devices (i.e., cell phone, satellite television receivers, microwave ovens, computers, radio towers) or other receivers when used in the same general geographic area.

The OM400 unit is not affected by the operation of other electronic devices or other receivers when used in the same general geographic area.

15. Each GPS tracking unit must be able to be electronically matched to any base station in the field-by-field personnel.

Since the OM400 device is a single unit device that is both the receiver of location information and the transmitter of status and location information, the device does not require a base or docking station or landline communications to transmit data. However, the OM400 RF Beacon is an *optional,* stationary, in-home monitoring device that can be paired with the OM400 GPS ankle bracelet to precisely verify home locations and extend valuable battery life. No active participation by the offender is required.

The OM400 RF Beacon uses radio frequency technology to provide the agency with an advanced solution to reliably monitor offenders in areas and environments where locations are problematic due to buildings or cellular coverage.


OM400™ RF BEACON

The OM400 RF Beacon offers the following features and benefits:

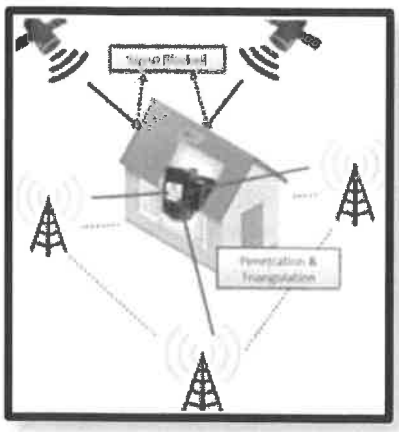
+ Accurately and reliably monitors curfews and reports all enters and leaves.
+ Monitors and reports A/C power disconnect, movement/relocation, and tampers.
+ Communicates over a proprietary encrypted signal to prevent false communication, jamming, and hacking.
+ Superior onboard memory in case of communication outage.
+ Internal backup battery lasts for up to 48 hours
+ Range of 150 feet

16. The GPS tracking unit should have a field replaceable battery. The battery should last for one year. Replacement batteries are at the expense of the Vendor.

The OM400 features an internal, rechargeable and non-removable battery that boasts one (1) of the industry's longest battery life of 12 to 18 months with a shelf life of three (3) years. Sentinel will replace the battery upon return to our warehouse and provide the Division with a replacement unit at no expense to the Division.

17. The GPS tracking unit should receive GPS signals in any spatial orientation.

The OM400 will send and receive signals within all plains of motion in any spatial orientation. The OM400 GPS units are always active and communicate through cellular coverage; therefore the unit is capable of monitoring an offender's movements at any time and in any location.



The OM400 uses both GPS and Advanced Forward Link Trilateration (AFLT) technologies to track offenders' locations. This dual-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking.

The OM400 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM400's unique design combines multiple layers of location technologies including AFLT (Advanced Forward Link Trilateration), GPS, and Assisted GPS (A-GPS). Such technology allows for reliable location information to be processed anywhere and compensate for poor GPS availability in GPS-impaired environments. The combination on these advanced location technologies

allows for the quickest acquisition time (typically within 60 seconds, so long as there a cellular signal detected) without an office being required to go outside to acquire a GPS signal when enrolling and installing a device.

The OM400 acquires GPS utilizing a system of satellites signals and, in the event the OM400 can only find a few GPS satellite signals due to partial blockage or location, it willautomatically shift to A-GPS. With A-GPS, the OM400 uses the available GPS signals in combination with cellular network data. In the instance of impaired GPS, or no GPS signal, the OM400 activates Advanced Forward Link Trilateration (AFLT). The AFLT triangulates utilizing ambient longitude and latitude data broadcast by the cellular environment. This is a unique capability and is possible with devices communicating via a CDMA cellular network.

The OM400 communicates via the **Verizon or Sprint** networks, both CDMA-based. Designed to track and allow communication with the offender 24/7, the OM400 locates indoors and out. As with typical GPS, interference is a reality and in any case, there are two (2) formats of signal that can be impacted; GPS and cellular signal. Such obstacles are geographic in nature (poor GPS location), signal disruptors (scramblers, shielding, tracing, and duplication), cellular turndown (termination of many 2G GSM networks as announced by AT&T), and locations with poor cellular reception. Taking these obstacles in mind, the OM400 technology is centered on reliably offering two (2) cellular networks - Verizon and Sprint - to heighten cellular options and provide reliable location data in GPS-impaired locations. The OM400 uses the CDMA wireless digital cellular standard to transmit and communicate data directly to the monitoring system via two (2) of the largest cellular networks in the world. The OM400 device uses encrypted communications that prevents tracing and duplication. Additionally, the OM400, through its CDMA communication capabilities, is not subject to the eminent, and in some cases immediate, "turndown of service" that has been announced by major GSM networks like AT&T. Therefore, there is no threat of interruption of service.

18. The GPS tracking unit must be able to store the number of events in memory and must have download capabilities so that agency staff can print hard copy status reports.

The OM400 GPS devices incorporate non-volatile memory so each device is capable of storing data indefinitely and printing hard copy status reports upon transmission to the monitoring system. The OM400 can store several days of tracking information in the on-board memory, regardless of the mode of operation, should the unit be unable to communicate with the monitoring application.

19. The Vendor must provide with the GPS system an ankle transmitter, which is capable of being worn by an offender in a comfortable, but secure manner at all times. The ankle transmitter must be attachable by a strap that is not abrasive to the offender's skin.

The OM400 GPS device is a one-piece, light-weight, ankle-worn GPS tracking solution that is both the receiver of location information and the transmitter of status and location information and does not require a separate tracking device to be carried. The unit is approximately 3.5 x 2.4 x 1.6 inches and weighs 8.4 ounces. The OM400 does not pose any known health or safety hazards to participants or other persons coming into contact with the tracking units. The OM400 transmitter case is made of Hypo-

Allergenic Acrylonitrile-Butadiene-Styrene (ABS) Plastic, a material that is durable and safe posing no hazard or danger to defendants. The device and all of its parts are FCC approved and/or certified in addition to meeting the UL Standards for lithium batteries, charger, and sharpness.

The devices are small, lights and do not inhibit participant activities. The OM400 device casings are hardened and waterproof in both salt water and fresh water. The units can withstand temperatures between -68° Fahrenheit and 140° Fahrenheit, and up to 500 MHz of random vibration of 1.25G rms. The OM400 will function under normal household, atmospheric and environmental conditions. The OM400 does not pose a safety hazard or unduly restrict the activities of the offender. It is also dishwasher safe, which is the easiest and safest way to sterilize the device.

---

20. Both the strap and ankle transmitter must be water resistant and capable of withstanding normal shocks, vibrations, and wear and tear. The ankle straps must come in various sizes or be adjustable to size to fit the offender.

The proposed device is truly 100% waterproof, safe to the wearer, engineered for heavy-duty shock resistance and FCC, CE, ROHS, IC and SAR compliant.

The OM400 strap is easily sanitized and reusable on multiple participants without the need for replacement. The device is attached to the participant's ankle with an extended length band to accommodate the largest of ankles. The strap's design allows for a secure fit and has multiple holes to assist in finding the proper fit on each person. The strap is adjustable as needed prior to locking the pins in place to allow the participant to stand up and/or walk around to determine the best fit possible.

---

21. Both the strap and the ankle transmitter must be tamper resistant so that the offender cannot remove it without an alert being sent to the Monitoring Center.

The OM400 unit will detect and report any attempts to cut, remove, or tamper with the strap attached to the device. When properly installed, attempts to defeat, remove or tamper with the OM400 GPS tracking device will also be visually obvious to trained personnel. The strap will show signs of cutting or dislodging as it is made of durable hypoallergenic materials that are molded into a uniform design. The back plate fits precisely in place and any attempts to pry it open are easily noticeable.

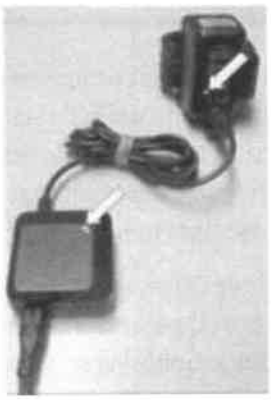
The OM400 GPS tracking device detects three (3) tamper types including 1) strap tamper, 2) device case tamper and 3) backplate tamper. Within one (1) second of a tamper attempt, the device will communicate and send a unique alert to the monitoring system web interface. The OM400 device will automatically and instantly communicate to the monitoring system software when a participant attempts to remove or tamper with the strap. The alert is received in real-time and provides an icon on the officer's dashboard as well as "popup" in a text list on the monitoring center application, providing both the officer and monitoring center with immediate visual identification of the tamper alert. The tamper icons on the dashboard do not automatically clear and must be manually cleared in the software.

The monitoring system then immediately sends the alert to the appropriate agency defined personnel. The elapsed time for a device tamper to be executed and then have a notification via text message and/or voice call is under 45 seconds. The OM400 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the back plate attached to the leg. Additionally, the unit will send a tamper alert if the unit is broken or if the unit's back plate is separated from the rest of the unit.

The OM400 is in full compliance with the "GPS Anti-Tampering Temporary Act of 2009", in that the OM400 is designed to detect and report any person required to wear a OM400 GPS device as a condition of supervision attempting to remove, intentionally alter, or interfere with or mask the operation of the device. In addition, the monitoring software application also has notifications to inform users if the device is not successfully locating or communicating due to a lack of available network or masking the device. Under these conditions, notifications for both the no communication and no location alerts can be sent to the monitoring center staff and/or officers for further investigation and designated in the system.

22. Battery life for the ankle transmitter battery should be noted in the proposal and it should be sufficiently durable to not require frequent replacement of the battery.

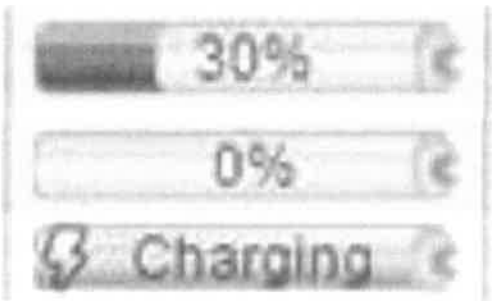
The OM400 features an internal battery that boasts one of the industry's longest battery lives of 12 to 18 months with a shelf life of three (3) years. Participants charge the unit through a standard 110V plug with a 15-foot cord easily connected directly to the front of the unit. The unit has an intensive monitoring battery up-time of up to 72 hours depending upon the rate plan used by the agency and is rechargeable in 1.5 hours. The OM400 features a multi-colored LED light that will illuminate during battery charging.



OM SERIES LED LIGHTS

Additionally, the device reports the battery status each time it reports to the monitoring center. If the device's power is low, the monitoring center will generate a low battery alert. A low battery alert is generally generated when the device is at 20% or less of battery power. This alert will clear when battery power is restored above 85%. To mitigate low battery issues, agencies can incorporate a mandatory recharging schedule into the participant's daily schedule. If the device is not charging at the

scheduled time, or if it is unplugged prior to the expiration of the charging schedule, the monitoring center can notify staff if required. The software also allows the agency to require the OM400 device to take specific action such as vibrating to alert the participant in the event of a low battery.



OM SERIES BATTERY STATUS

23. The Vendor must furnish the necessary tools to attach and removal of the ankle transmitter and/or straps at no additional cost to the Division.

Sentinel will provide the necessary tools and straps to attach and remove the ankle-worn OM400 GPS tracking unit at no additional cost to the Division.

E. ANKLE TRANSMITTER RF

1. The ankle transmitter shall attach around the ankle of the offender and shall be lightweight.

The RF Patrol PTX2 (transmitter) is 1.57 X 2.72 X 0.77 inches and weighs 1.51 ounces. The unobtrusive, hypoallergenic, and sleek bracelet design makes it one of the smallest body-worn bracelets available on the market. It is easily, securely, and comfortably attached to the ankle of participants under normal slacks. It is moisture and waterproof, shock resistant, unaffected by normal human environmental and atmospheric conditions, and does not pose a safety or health threat to the wearer or unduly restrict the activities of the participant. Sentinel provides varying length straps designed to fit any ankle size.

2. The ankle transmitter shall send an individually coded signal (no duplication), which has an adjustable range between 50-150 feet and is user defined.

The RF Patrol transmitter emits a unique, constantly changing signal three (3) times per minute. Each time the bracelet transmits its signal, it reports the serial number of the transmitter associated to the participant, its power status, and tamper status.

The bracelet records and reports each tamper as a separate event alerting the agency of a participant's tamper frequency level. The RF Patrol monitoring system's signal range is agency programmable and

variable with three (3) settings as follows:

- Low, approximately 50 feet
- Medium, approximately 100 feet
- High, approximately 150 feet

RF Patrol features a programmable leave window at the participation agency's direction either all units shipped to an agency or on a per unit/participant basis. The standard leave window is five (5) minutes, but can easily and remotely be adjusted.

—IMPORTANT SENTINEL ADVANTAGE—
Sentinel's unique dual transceiver approach incorporates both a transmitter and receiver in the home unit, as well as having both in the transmitter. In fact, the RF Patrol home unit has two (2) constantly active internal antennas capable of both receiving from and transmitting signals to the bracelet to maximize the ability to detect the presence of transmitter signals. 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. This enables RF Patrol to provide the most accurate RF signaling and fastest notification on the market.

---

3. The ankle transmitter and strap must have dual tamper resistant features that will enable the transmitter to immediately notify the monitoring center of any tamper attempt or removal from the offender's ankle utilizing fiber optics. This would include severing the strap or removal of the transmitter without severing the strap.

The RF Patrol transmitter (bracelet) has a highly advanced tamper detection scheme that will detect when an attempt is made to cut or remove the advanced fiber-optic detection strap from the participant's ankle transmitter.

The 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. If a participant attempts to cut the fiber-optic strap or remove the unit, the unit automatically activates a "tamper alert" signal and transmits the "tamper alert" to the home monitoring unit three (3) times per minute while in range. Sentinel bracelets 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.

Sentinel provides varying length straps designed to fit any ankle size. When properly installed, participants cannot remove the bracelet without destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot stretch or slip off the bracelet 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