

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS	2
II. RESPONSE TO TECHNICAL CRITERIA	23
A. SCOPE OF WORK – CATEGORY 1: GPS	24
A. GPS Hardware	24
B. GPS Software	42
C. GPS Customer Support & Training	82
Remaining Category 1: GPS Questions	86
B. SCOPE OF WORK – CATEGORY 2: RF	180
A. RF Hardware	181
B. RF Software	190
C. RF Customer Support & Training	201
Remaining Category 2: RF Questions	205
C. SCOPE OF WORK – CATEGORY 3: ALCOHOL MONITORING	250
A. CAM OR TAC	251
1. CAM Hardware	251
2. CAM Software	256
3. CAM Customer Support and Training	263
B. REMOTE ALCOHOL MONITORING (RAM)	267
1. BAT Hardware	267
2. BAT Software	277
3. BAT Customer Support and Training	279
Remaining Category 3: Alcohol Monitoring Questions	283
D. CUSTOMER SATISFACTION	317
E. SOFTWARE INTEGRATION	321
F. ARTIFICIAL INTELLIGENCE	322
G. SUPPLY CHAIN	322
H. QUALITY ASSURANCE AND HARDWARE RETURNS	323
I. IMPLEMENTATION AND PROMOTION OF NASPO	325
SUPPORTING DOCUMENTATION	340



Attachment 08

OFFEROR RESPONSE WORKSHEET

Offeror must provide complete and succinct responses to each item below. **Insert your responses into this worksheet directly below each question or prompt.** While supplementary marketing materials are neither requested nor desired, Offeror should provide all information necessary to demonstrate Offeror's ability to meet the requirements of this RFP and the RFP's Scope of Work.

I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS

I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS

- A. OEM (Original Equipment Manufacturer) must have three (3) years' experience demonstrating the ability to provide the Electronic Monitoring equipment and monitoring services to the criminal justice marketplace. Offerors must respond with a written narrative confirming three (3) years' experience.

SENTINEL RESPONSE

Sentinel is the Original Equipment Manufacturer for our RF Patrol and our OM Series GPS solution. We have been providing offender monitoring services for 32+ years, Global Positioning Satellite System (GPS) equipment and tracking services for 28 years, and we have been providing Alcohol Monitoring Services for 31 years.

Sentinel has contracted with some of the most progressive and demanding correctional agencies in the provision of electronic monitoring, including for the services of radio frequency electronic monitoring, GPS tracking, and alcohol monitoring. Today, we serve correctional agencies at all levels of government. This entails state-level agencies that include the State of Alabama Bureau of Pardons & Paroles, the State of Connecticut Judicial Branch, the State of New Hampshire Department of Corrections, and the State of Hawaii Judiciary and Department of Public Safety. In addition, we are contracted with some of the largest county programs in the country including operations in Leon and Miami-Dade Counties within Florida; Bexar, Dallas, and Harris, Counties within Texas; Los Angeles, San Diego, and San Francisco Counties within California; Dauphin County and the City of Philadelphia within Pennsylvania; and in the Cities of Seattle and Tacoma, Washington, just to name a few. Sentinel also provides state-of-the art technology and services at the federal level including the District of Columbia Pretrial Services Agency and the District of Columbia Superior Court.

Sentinel's performance for these agencies, as well as to all our customers nationwide, demonstrates that we execute upon our commitment to providing services that meet or exceed the equipment and distinct service needs for each program. In addition, over the last 32+ years, we have gained unparalleled knowledge and experience in how to successfully design, implement, and operate programs that are based on clear communication and strict compliance with program requirements, and we are focused on providing the highest-level services to our customers.

As one of the nation's leading providers of electronic monitoring/offender services, with twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement #22PSX0021, Sentinel has unparalleled experience in electronic monitoring and more specifically in successfully marketing NASPO ValuePoint cooperative contracts. Additionally, under our current NASPO ValuePoint Contract #22PSX0021, Sentinel provides numerous Participating Entities services in all three (3) technology categories:

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Category 1: Radio Frequency Monitoring
- + Category 2: Alcohol Monitoring
- + Category 3: GPS Satellite Monitoring
- + Each category additionally encompassing Optional Contractor Provided Services

As a longer-term partner to NASPO, Sentinel has truly demonstrated and proven to serve as an "all-inclusive solutions and services provider." We stand ready to continue providing services for the new Electronic Monitoring contract with technology and services to meet all categories required.

Sentinel also has an extensive relationship with Alcohol Monitoring Systems Inc. (AMS) dba SCRAM Systems, the manufacturer of the proposed SCRAM Continuous Alcohol Monitoring (SCRAM CAM) bracelet that provides 24/7 transdermal alcohol testing for hardcore drunk drivers and/or repeat high-risk alcohol offenders as well as the Remote Breath Pro handheld portable breath alcohol testing unit. As an AMS-authorized Service Provider, Sentinel is a direct extension of AMS and the hands-on representative in the field, offering comprehensive, responsive, and valuable services to Agencies. Sentinel's staff have undergone extensive training in every facet of SCRAM Systems operations and has undergone an extensive AMS certification process, so the result is best-in-class program development, excellent service execution, and technical innovation.

Our collaboration includes SCRAM Systems providing certified data analysts to review all CAM alcohol monitoring alerts with no need for the agency staff to initiate or request confirmation results, thereby, reducing officers/agency workloads. The collaboration between Sentinel and SCRAM Systems will provide Participating Agencies single-source admissibility. When an alert is detected, SCRAM Systems analysts analyze seven (7) individual pieces of criteria to determine if consumption has taken place, including equations to determine absorption and elimination rates, sample contamination, as well as characteristics to determine when a consumption event begins and ends. In addition, the review process identifies the presence of environmental alcohol and looks at key characteristics of the Transdermal Alcohol Concentration (TAC) curve to ensure that only true drinking episodes are confirmed. This process has been validated in numerous court hearings to date and Sentinel has worked with SCRAM Systems for more than 18 years in the provision of SCRAM devices to some of the largest alcohol monitoring programs in the United States.

Additionally, Sentinel is an authorized Value-Added provider of the Shadowtrack Technologies ShadoWatch, a wrist-worn GPS device, and Shadowtrack mobile applications. Sentinel has successfully deployed these services throughout the United States. ShadoWatch is the latest advancement and product offering in the offender electronic monitoring industry and offers agencies a wrist-worn GPS device for monitoring and supervising low- to moderate-risk clients assigned to electronic monitoring or for those who are unable to wear an ankle device for medical reasons. ShadoWatch is a discreet wrist-worn one-piece GPS tracking device that helps properly monitor program participant compliance. Also used for low and moderate risk program clients, the Shadowtrack mobile applications utilize the client's mobile phone to allow the participant to check-in remotely as required by the agency, report on their schedules, provide confirmation of location, and directly communicate with agency officers. Our relationship with Shadowtrack provides for the utilization of ShadowBriety, a comprehensive supervision tool designed for participants required to submit to alcohol testing featuring bluetooth and facial recognition technology. Please reference the **Supporting Documentation** (page 340) section of this Attachment for copies of **Letters of Support from SCRAM Systems and Shadowtrack Technologies**.

It is important to note that Sentinel, as the prime contractor for any contracted services performed, maintains 100% responsibility. Sentinel **owns and operates** our National Monitoring Centers located in Norco, California, and Atlanta, Georgia. Our monitoring centers are staffed with Sentinel dedicated employees 24 hours a day, seven (7) days a week, 365 days a year with trained personnel and supervisors available on every shift. To additionally aid our eastern customers, Sentinel also has a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia 30005. **With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers.**

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- B.** Offeror must declare that all current products and services meet CJIS and FCC requirements as referenced in Attachment 02, SOW. Offerors must respond with a written narrative confirming CJIS and FCC requirements are being met.

SENTINEL RESPONSE

As outlined in Attachment 02, Scope of Work_Revised 2-6-26~2, item I.B, which states, "*All proposed tracking systems must adhere to the National Institute of Justice, Standard Offender Tracking Systems, 1004.00. All equipment (new or used) must be properly registered and certified under the Federal Communication Commission ("FCC") rules and regulations, as applicable.*", Sentinel is confirming products and services adhere the National Institute of Justice Standard Offender Tracking Systems 1004.00 and are Federal Communication Commission ("FCC") certified. Note, Sentinel staff participated in the development of Offender Tracking Standards at the time of creation. Moreover, out of an abundance of caution and while not a requirement, Sentinel has designed our systems, operations, and policies to align with Criminal Justice Information Services (CJIS) requirements.

Additionally, as outlined in Attachment 02, Scope of Work_Revised 2-6-26~2, item I.B, in the event any component of Sentinel's service becomes inoperable, Sentinel will immediately notify the Participating Entity Representative(s) or designees by telephone or more expedient means available, but no later than sixty (60) minutes after service failure.

Sentinel's proposed equipment has been properly registered and certified under Federal Communications Commission (FCC) rules and regulations. Please reference the **ISO 9001:2015 Certificate** included in the **Supporting Documentation** (page 340) section of this Attachment confirming Sentinel's ISO certification as well as the **Federal Communications Commission Certificates** confirming certification for the proposed equipment.

EQUIPMENT TYPE	FCC CERTIFICATION
OM500 Tracking Device (transceiver)	TS5-WP76-OM500
OM500 Beacon	TS5-OM500B
RF Patrol Ankle-Worn Transceiver	NSNPTX08
RF Patrol Receiver / Home Monitoring Unit – Cellular	NSNPHMUC08
RF Patrol Receiver / Home Monitoring Unit – Landline	NSNPHMUL08
RF Patrol Receiver / Home Monitoring Unit Lock	NSNOPID08
SCRAM II Transdermal Alcohol Monitoring Bracelet	P8M-SM02
SCRAMx Transdermal Alcohol Monitoring Base Station - Landline	P8M-SM03
SCRAMx Transdermal Alcohol Monitoring Base Station – Ethernet	P8M-BS400
SCRAMx Transdermal Alcohol Monitoring Base Station – Cellular	P8M-BS500
SCRAM Remote Breath Pro	P8M-RB200
ShadoWatch	2ARH7-W-N70ST
ShadowBriety - BACtrack	S8B-M5



- C. Offeror must provide Nationwide Services (including Hawaii and Alaska). Offerors must describe their ability to provide services outside of the United States, e.g. US Territories and Canada. Offerors must respond with confirmation of Nationwide Services, and their ability to provide services outside of the United States.

SENTINEL RESPONSE

Sentinel has and will continue to provide delivery and service continuity of all Products and Services proposed and awarded under the Master Agreement to all fifty (50) states, including Hawaii and Alaska as well as the District of Columbia and U.S. territories, and all of Sentinel's brick and mortar locations, including our data centers, are based, staffed, and operated in the United States.

Sentinel **owns and operates** our National Monitoring Centers located in Norco, California, and Atlanta, Georgia. The Norco Monitoring Center will serve as the focal point for all proposed technologies and all proposed services thereby providing maximum continuity of service delivery to all Participating Entities. The primary monitoring center is the focal point of Sentinel's state-of-the-art facility, located in Norco, California that is staffed with Sentinel dedicated employees 24 hours a day, seven (7) days a week, 365 days a year with trained personnel, from which Sentinel handles over 50,000 calls daily. This is the central location from which all monitoring center activities are conducted, and information is disseminated to the agencies that we provide services. The Atlanta monitoring center will continue to support daily alert management tasks and serve as a backup center in the event of an interruption in Norco.

Sentinel is able to deliver devices quickly and affordably due in large part to our available inventory and use of two geographically separated warehouses. Our distribution warehouse in Anaheim, California, along with our Alpharetta, Georgia warehouse ship equipment daily to our customers. This regional distribution model minimizes costs and eliminates unnecessary delays.

Sentinel employs a staff of nearly 290 employees located throughout the United States, and we operate offices in approximately 20 different locations; our Monitoring Center staff is decentralized and staffed across the United States so telephone impact due to a single location or entire geographic zone is minimized. Our nationwide footprint, with current service offerings in more than 40+ states, has allowed us to meet the needs of our customers regardless of their geographic location.

Sentinel is one of the nation's leading providers of electronic monitoring/offender services, with twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement #22PSX0021, Sentinel has unparalleled experience in electronic monitoring and more specifically in successfully marketing national NASPO cooperative contracts. Additionally, for NASPO RFP #22PSX0021, Sentinel was awarded a NASPO ValuePoint cooperative contract in all three (3) technology categories:

- + Category 1: Radio Frequency Monitoring
- + Category 2: Alcohol Monitoring
- + Category 3: GPS Satellite Monitoring
- + Each category additionally encompassing Optional Contractor Provided Services

Sentinel has truly demonstrated the ability to support programs throughout the United States and has scaled our operations to support the growth experienced by our customers over the last five years.



- D. Technology.** Offerors must provide the necessary documentation to meet the Information Technology Security Requirements in Attachment 02, III. Offerors who fail to meet this requirement will be deemed non-responsive. Offerors shall describe the measures taken to protect sensitive Participating Entity and Client information.

SENTINEL RESPONSE

The system's security and data-management framework is aligned with criminal-justice security expectations, providing full traceability for evidentiary purposes and long-term data retention requirements as required in item III. Information Technology Security Requirements, Attachment 02, Scope of Work_Revised 2-6-26~2.

As a leading provider of electronic monitoring programs for nearly 33 years and as the most active Contractor on NASPOValuePoint Master Agreement 22PSX0021, Sentinel recognizes the importance of maintaining robust security protocols and continual security improvement. Sentinel policies are based on NIST SP 800-53. Sentinel's security staff members have worked within the NIST 800-53 related standards and frameworks for 12 17 years and have received accreditation for NIST 800-53 compliance for past contracts and products. Every member of Sentinel's cybersecurity staff has more than 20 years of experience. Sentinel's security operations partners have experienced staff that include direct federal cybersecurity employment. Both Sentinel and partners have decades of experience with handling sensitive information.

The Sentinel proposed monitoring applications operate in a secure, highly reliable, redundant, and scalable infrastructure. The data center environment was designed with security, redundancy and continuous operations in mind at every layer. In addition to steps taken to detect and prevent misuse or tampering of Sentinel's products and services, the platform is deployed at multiple data centers to provide geographical redundancy. Data is continuously replicated from the Primary to the Secondary data center providing failover redundancy whenever needed. The infrastructure is designed with high-availability storage area networks. The datacenter operations are monitored and supported by Sentinel employed hardware and software engineers 24/7/365 to ensure continuous operation and maximum uptime.

Sentinel's Primary Monitoring Systems are located in a SOC 2 Type II audited datacenter in Los Angeles, California and the FedRAMP listed Oracle Government Cloud datacenter in Ashburn, Virginia. Sentinel's Secondary Monitoring Systems are located in a SOC 2 Type II audited datacenter in Dallas, Texas and the FedRAMP listed Oracle Government Cloud datacenter in Phoenix Arizona. All datacenters hosting the Monitoring Systems possess multiple disaster mitigation features with fire suppression systems, UPS and Generator protected electrical, and strict policies and procedures for access control. The monitoring centers meet all applicable federal, state, and local regulations regarding safety, including building codes regarding earthquake and hurricane resistance.

III. Information Technology Security Requirements. (Applies to all categories)

- A.** The Contractor must be AICPA SOC 2 compliant covering all five (5) functional areas (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a third-party assessment based on current revision of NIST 800-53 Moderate controls conducted within the last two (2) years, or FedRAMP authorization, or GovRAMP authorization, or equivalent. This is a mandatory requirement of the RFP; Offerors who fail to adequately demonstrate their security standards may be deemed non-responsive. The Contractor must keep all information regarding the Purchasing Entity, Clients, whether obtained from the Purchasing Entity, from Eligible Persons, or through performance of the services under the Master Agreement, confidential and secure and additionally must dispose of all information in a manner that meets or exceeds the AICPA SOC 2 standards.

SENTINEL RESPONSE

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Sentinel's industry-approved approach combines encryption technologies, security, and regulatory compliance frameworks that meet the security standards required by this RFP.

Sentinel maintains an aggressive posture of cyber security diligence with an ongoing focus on continuous improvement of security operations. Components of Sentinel's applications are hosted in the Oracle Government Cloud Infrastructure. The U.S. Department of Defense, intelligence community, and federal civilian agencies rely on Oracle Government Cloud. Oracle US government cloud infrastructure meets the standards DoD DISA IL 5, 4, 2, FedRAMP-High, FIPS 140-2 for cryptographic modules and is VPAT section 508 compliant. Sentinel's security and data management framework are aligned with criminal justice security expectations, providing full traceability for evidentiary purposes and long-term data retention requirements. Most recently evidenced through our award of the Harris County, TX Request for Proposal, which included review and approval of Sentinel's Information Security (Cybersecurity) Controls. Sentinel maintains compliance with applicable federal, state, and local data protection laws. Our systems support audit trail generation and configurable data retention policies.

The Sentinel proposed monitoring applications operate in a secure, highly reliable, redundant, and scalable infrastructure. The data center environment was designed with security, redundancy and continuous operations in mind at every layer. In addition to steps taken to detect and prevent misuse or tampering of Sentinel's products and services, the platform is deployed at multiple data centers to provide geographical redundancy. Data is continuously replicated from the Primary to the Secondary data center providing failover redundancy whenever needed. The infrastructure is designed with a high-availability storage area network (SAN) containing redundant and automatic iSCSI pathing across multiple network interfaces, multiple network switches, and all flash SAN storage managed by redundant SAN controllers. The system is monitored and supported by Sentinel staff 24/7/365 to ensure continuous operations, and maximum uptime.

Sentinel's Primary Monitoring Systems are located in a SOC 2 Type II audited datacenter in Los Angeles, California and the FedRAMP listed Oracle Government Cloud datacenter in Ashburn, Virginia. Sentinel's Secondary Monitoring Systems are located in a SOC 2 Type II audited datacenter in Dallas, Texas, and the FedRAMP listed Oracle Government Cloud datacenter in Phoenix, Arizona. All datacenters hosting the Monitoring Systems possess multiple disaster mitigation features with fire suppression systems, UPS and Generator protected electrical, and strict policies and procedures for access control. The Sentinel monitoring centers meet all applicable federal, state, and local regulations regarding safety, including building codes regarding earthquake and hurricane resistance.

Sentinel's Data Centers are located in secured locations with security provisions where access to computer records is restricted to authorized individuals. The Sentinel proposed monitoring application (DNA) operates in data centers that are a minimum of SOC 2 Type II audited with strict access controls.

The DNA Monitoring Application and Case Management Software were designed and are managed based on following NIST SP 800-53 requirements. Sentinel's security staff members have worked within the NIST 800-53 related standards and frameworks since 2009 and have received accreditation for NIST 800-53 compliance for past contracts and products.

The Company enforces role-based access control (RBAC) for access to systems and data through centralized identity and access management. Access is granted only to pre-defined roles aligned to job responsibilities and the principles of least privilege and need-to-know, with documented approval from designated system/data owners. Privileged and administrative access is tightly restricted (including the use of MFA for privileged and remote access), and role assignments are reviewed at least quarterly and upon personnel or job changes, with prompt removal upon termination. Access provisioning, changes, and administrative actions are logged and monitored to support auditability and align with NIST SP 800-53 Moderate access control objectives (e.g., AC-2, AC-3, AC-5, AC-6).



SENTINEL THIRD PARTY ASSESSMENT

Sentinel's most recent independent penetration test and third-party vulnerability assessment was completed in April 2025 by ARCTIQ, a cybersecurity professional services firm specializing in governance, risk, and compliance. The engagement included scoped adversarial testing and vulnerability validation to identify exploitable conditions and control gaps, and to produce risk-ranked findings and remediation guidance. Consistent with NIST SP 800-53 requirements for independent assessment and vulnerability management, Sentinel triages findings based on severity and likelihood, assigns remediation owners and due dates, and tracks corrective actions to closure. Sentinel then validates remediation through follow-up evidence review and targeted retesting with ARCTIQ to confirm vulnerabilities have been effectively remediated and are no longer reproducible.

SENTINEL CYBERSECURITY

Sentinel partners with Arctic Wolf to deliver Security Operations Center services, Managed Detection and Response, Managed Security Risk, and Managed Security Awareness, and uses SentinelOne for XDR endpoint protection across all endpoints. Arctic Wolf operates a Security Information and Event Management platform that aggregates and correlates telemetry from across the Sentinel environment, including Arctic Wolf Managed Detection and Response and SentinelOne XDR endpoint agents, network equipment telemetry and packet-level network inspection, internal and perimeter firewall traffic and audit logs, access and authentication logs, Microsoft 365 access and email auditing, and security auditing and logging from other cloud providers. This consolidated monitoring and analysis provides both Arctic Wolf and the Sentinel Cyber Security Team with tactical and historical awareness to support rapid 24x7 managed detection and response when threats are identified, as well as ongoing threat hunting and security auditing across the enterprise. In coordinated operation with Sentinel's internal and perimeter firewalls, these capabilities support detection and prevention of malicious activity, including intrusion attempts, malware and ransomware behavior, suspicious traffic patterns, account takeover indicators, and potential lateral movement.

Arctic Wolf's Managed Security Risk includes Managed Risk Continuous Vulnerability Scanning and continuous vulnerability assessment across external public-facing and internal attack surfaces, enabling prioritized remediation, continued hardening, and defense of critical information systems.

SentinelOne XDR provides endpoint protection against intrusion, malware, ransomware, and anomalous behaviors, including automated protection and response actions when high-severity incidents are detected. Sentinel's staff and security partner also monitor security bulletins and threat intelligence sources for emerging threats, zero-day vulnerabilities, and newly disclosed Common Vulnerabilities and Exposures with immediate prioritization for remediation, and review relevant breach sources, malicious-actor forums, and known breach databases for any indication of Sentinel-related exposure or compromised credentials. Sentinel further strengthens its human defenses through continuous Managed Security Awareness training, testing, and phishing simulations with required remediation for all employees, and maintains an incident response retainer and cybersecurity warranty through Arctic Wolf in addition to existing cyber coverage.

Sentinel protects the perimeter of the data center and office networks with Fortinet FortiGate firewalls with Intrusion Detection and Intrusion Prevention features enabled and tracked. Security and Traffic activity is logged and ingested into the Arctic Wolf SIEM for combined Managed Detection and Response (MDR). Combined with the SentinelOne XDR Endpoint Protection Platform that runs on all Sentinel's servers and employee workstations and laptops, the Arctic Wolf 24x7 operated MDR service provides 24x7 rapid detection and reaction to intrusions.

Sentinel does not allow vendors or 3rd party access to participant data. Sentinel staff and end users (agency officers) access participant data using multi-factor authenticated access. All activities conducted in DNA are recorded with date, time stamp, and user credentials to provide audit capability, replay of events, and access to historical accuracy.



SENTINEL PERSONNEL SECURITY

Only authorized personnel assigned to our National Monitoring Centers and specific privileged staff in our IT Group have access to program participant data, and monitoring center personnel are unable to modify or alter monitoring data. At no time will we ever disclose confidential data to any unauthorized personnel without written approval of the participating agency or by an officer providing a confidential verbal password. All program data is maintained in accordance with industry-accepted secure data protection standards. The only staff members who are authorized to access or receive information on program participants are those who have undergone a background check and are assigned to support 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 assigned to the monitoring center and IT Group is required to undergo a thorough background check (including drug testing) and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements will result in the termination of the employee's employment.

Further, upon hiring, all our employees are provided with an employee handbook that outlines Sentinel's "zero tolerance" policy regarding compromising relationships with participants, their families and customer staff. We will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the operational management contact of the participating agency.

SENTINEL SECURITY OF MONITORING RECORDS

Access to the Monitoring System websites, systems, privileged access, and administrative consoles is protected by multi-factor authentication. Customer access is protected by multi-factor authenticated Single Sign On. Sentinel Staff with privileged access to the system gain access over a multi-factor authenticated Client VPN. IPsec tunnels between sites are secured based on NIST SP 800-77 rev 1 specifications.

Each authorized user is provided with their own login and once they have established their confidential password, Sentinel is able to ensure the integrity of each user's entry. This unique user access permits our Information Technology personnel to follow electronic audit trails that permit supervisors and management to verify the source of all data entries or modifications. Monitoring System Passwords are stored using salted, memory-hard hashing (Argon2id, per RFC 9106); plaintext passwords are never stored.

All records created for participants referred to this program will remain the property of the participating agency and will not be released without the written consent of the agency or due to compliance with a legal subpoena. Upon completion of services, all records are returned to the participating agency or destroyed under direction of agency-authorized personnel in accordance with agency requirements that meet or exceed required standards. Additionally, Sentinel encrypts all data backups with keys that only select IT Operations staff can access.

NOTE: No participant data is stored on the hard drive of a computer accessing the monitoring system (internally or externally). In the event of the theft or destruction of a computer that has accessed our system, confidential participant data and records will not be compromised. All data is stored on our secure servers in our Primary sites in Los Angeles, California, and Oracle Cloud Ashburn, Virginia, and Disaster Recovery sites in Dallas, Texas, and Phoenix, Arizona.

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, we have taken precautions to ensure the integrity and security of our system with protection of records and their confidentiality are our primary concerns. All our security systems are monitored electronically and manually by our IT group continuously to ensure no lapse in service.

To aid in the integrity of records, Sentinel uses Intrusion Detection and Intrusion Prevention at perimeter firewalls, combined with XDR endpoint agents and MDR endpoint agents installed on every system and workstation. This data is collected into the Security Information and Events Management system operated by a 3rd party Security Operations Center that monitors the system 24x7 both manually and with automation for detected threats.



Sentinel staff is immediately informed of suspicious activity on files and systems.

SENTINEL MONITORING SYSTEM SECURITY

Access to the Monitoring System websites, systems, privileged access, and administrative consoles is protected by multi-factor authentication. Customer access is protected by multi-factor authenticated Single Sign On. Sentinel Staff with privileged access to the system gain access over a multi-factor authenticated Client VPN. IPsec tunnels between sites are secured based on NIST SP 800-77 rev 1 specifications.

The Monitoring Center systems and servers use a minimum of TLS 1.2 with best practice cryptographic ciphers and modules based on FIPS 140-3 and NIST SP 800-52 Rev 2 for all HTTPS access to monitoring applications and for Data in Transit. Data at rest is encrypted using AES-256 and remains encrypted before being transmitted. If industry best practices are updated due to weaknesses being identified in any federally compliant ciphers and modules, Sentinel implements them based on severity without waiting for federal standards publications to be revised.

The system is continuously synchronized and replicated in its entirety to secondary offsite Disaster Recovery systems, in addition to all data being backed up and encrypted for off-site long-term storage.

All changes to participant or demographic information or monitoring data are saved within the system. Additionally, each employee has a specific database login credential that permits Sentinel to perform detailed audits on user access to all participant records in the database to confirm that unauthorized changes have not been made.

Our IT staff has installed all of the necessary physical and technical security measures (e.g., TLS certificates, network firewalls, Endpoint Protection providing protection from malware and ransomware, Monitoring Agents for Managed Detection and Response, access control equipment) to ensure that unauthorized users and malicious actors do not have access to Sentinel's information technology infrastructure, applications, data or our National Monitoring Center facilities.

SENTINEL INCIDENT RESPONSE AND BREACH NOTIFICATION

Sentinel maintains documented incident response procedures. In the event of a suspected or confirmed security incident or data breach, we will notify affected Participating Entities immediately and in no event more than 24 hours following discovery. We maintain cyber liability insurance coverage meeting the requirements specified in this RFP.

SENTINEL PHYSICAL SECURITY

Sentinel's Primary and Disaster Recovery data centers are a minimum of SOC 2 Type II audited secure facilities with strict policies and procedures for access control and video surveillance. All data centers have redundant electrical, HVAC, and UPS, with generator backup.

The Monitoring Centers meet all applicable federal, state, and local regulations regarding safety, including building codes regarding earthquake and hurricane resistance. For security purposes, our Monitoring Center sites do not conduct any business with the general public as it contains our corporate office and Monitoring Center Operations. Program participants do not have access to our facilities.

Our monitoring centers restrict data access to authorized staff by enforcing an electronic card key system for entryway access to the building and monitoring center facility.

The Primary Monitoring Center is located in our Norco corporate facility in California, and our Secondary center is located in our Atlanta, Georgia facility.



SENTINEL DEVICE ENCRYPTION

OM500 Encryption: Communication between the OM500 device and the Sentinel platform is secured using TLS 1.2, ensuring all data transmitted between the device and the platform is encrypted in transit. In addition to transport-layer encryption, an application-layer encryption scheme is implemented using a unique AES-GCM-256 key assigned to each device, providing device-level authentication and ensuring data originates from the intended device.

All SMS communications to and from the device are encrypted using AES-GCM-256, with Base64 encoding applied for secure transmission over the SMS channel. The OM500 operates within a private IP address pool, preventing direct internet access to the device, and peer-to-peer IP communication between devices is blocked. Device identity used for authentication and communication is derived from secure elements within the cellular module.

At the radio layer, LTE Cat 1 security in the United States uses AES-128 (128-EEA2) for air-interface confidentiality, AES-CMAC 128-bit (128-EIA2) for signaling integrity, and SIM-based EPS-AKA for mutual authentication.

RF Patrol Encryption: 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. RF transmissions are the most reliable, sophisticated, and highly encrypted in the industry. 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.

SCRAM SYSTEMS SECURITY

SCRAM Systems maintains a comprehensive security posture designed to protect sensitive client and Participating Entity data throughout its lifecycle. Their approach combines industry-standard certifications, encryption technologies, and regulatory compliance frameworks that meet and exceed the security standards required by this RFP.

SCRAM Systems meets the Information Technology Security Requirements of this RFP through TX-RAMP Level 2 certification demonstrating NIST 800-53 Moderate compliance, supplemented by ISO 27001 and ISO 27701 certifications and SOC 2 certified infrastructure. The layered security architecture provides encryption in transit and at rest across all system components, and the digital chain of custody framework has supported successful evidence admission in courts nationwide. Their data center and cloud infrastructure providers maintain SOC 2 Type II compliance.

SCRAM SYSTEMS SECURITY CERTIFICATIONS AND STANDARDS

Upon request, SCRAM Systems will provide copies of their TX-RAMP Level 2 certification, ISO 27001 and ISO 27701 certificates, and infrastructure provider attestation letters.

SCRAM SYSTEMS DATA PROTECTION ARCHITECTURE

SCRAM Systems employs a layered security architecture appropriate to each component of their monitoring solutions.

SCRAM CAM (Continuous Alcohol Monitoring): The SCRAM CAM bracelet communicates with the base station using encrypted radio frequency (RF) transmission. The base station connects to SCRAM's backend systems through multiple connectivity options including Ethernet, Wi-Fi, cellular (LTE), or landline, depending on installation requirements. When cellular connectivity is used, data benefits from carrier-standard LTE encryption.



The bracelet maintains up to 30 days of on-device data storage, and the base station maintains approximately one month of data storage, ensuring data integrity is preserved even during temporary connectivity interruptions.

SCRAM GPS (Location Monitoring): The SCRAM GPS 9 Plus bracelet communicates via the FirstNet wireless network using 4G/LTE connectivity. LTE provides radio-link encryption using AES-based cipher profiles (128-EEA2 for confidentiality, 128-EIA2 for integrity). The device holds FirstNet Trusted designation, indicating completion of extensive cybersecurity and connectivity testing for IoT devices. When the optional SCRAM Beacon is deployed for home monitoring scenarios, the bracelet communicates with the Beacon using a proprietary RF protocol. The device maintains on-board zone storage, enabling local detection and recording of location violations regardless of connectivity status.

Web-Based Platforms: All SCRAM web-based monitoring platforms, including SCRAM Optix and related software, are protected by TLS encryption for all user sessions. Role-based access controls govern data access, with authentication required for all system access. Administrative access is logged and auditable.

Data at Rest: All client data stored in SCRAM databases is encrypted at rest using industry-standard encryption, protecting against unauthorized access at the storage layer.

SCRAM SYSTEMS DIGITAL CHAIN OF CUSTODY

SCRAM Systems employs a comprehensive digital chain of custody framework designed to produce reliable evidence for court proceedings. This framework includes:

Secure Data Collection: Data is collected directly from monitoring devices through secured communication channels. SCRAM CAM uses encrypted RF transmission to the base station. SCRAM GPS uses LTE encryption via the FirstNet network. Both systems maintain on-device data buffering (up to 30 days for CAM, on-board storage for GPS) to ensure data integrity during connectivity interruptions.

Digital Logs and Tracking: All system access and data modifications are logged with timestamps and user identification. Audit trails are maintained in accordance with regulatory requirements and support forensic review when needed.

Tamper-Proof Storage: Stored data is protected through encryption at rest, role-based access controls, and comprehensive audit logging. Any access to or modification of stored data is recorded.

Access Control: SCRAM platforms enforce role-based access controls ensuring that users access only the data and functions appropriate to their role. Multi-factor authentication is available for enhanced security.

System Integrations: SCRAM systems support secure integration with Participating Entity systems through documented APIs and secure data exchange protocols.

Tamper Detection: SCRAM devices incorporate sophisticated tamper detection mechanisms. SCRAM CAM performs tamper checks during each reading cycle and can detect attempts to obstruct or remove the device. SCRAM GPS includes strap tamper detection using embedded fiber optic technology, GPS jamming detection, and additional sophisticated detection mechanisms to identify device compromise attempts.

SCRAM SYSTEMS REGULATORY COMPLIANCE

SCRAM Systems maintains compliance with applicable federal, state, and local data protection laws. Our systems support audit trail generation and configurable data retention policies to meet Participating Entity requirements.

SCRAM Systems' security architecture is designed to align with CJIS Security Policy technical controls. While they do not currently hold CJIS certification, their infrastructure and practices are capable of supporting CJIS compliance should a Participating Entity provide the requisite sponsorship arrangement.



SCRAM SYSTEMS INCIDENT RESPONSE AND BREACH NOTIFICATION

SCRAM Systems maintains documented incident response procedures. In the event of a suspected or confirmed security incident or data breach, we will notify affected Participating Entities immediately and in no event more than 24 hours following discovery. We maintain cyber liability insurance coverage meeting or exceeding the requirements specified in the RFP.

SHADOWTRACK SECURITY

Shadowtrack utilizes SOC 2, Type II Compliance to further mitigate risk and to help keep agency's sensitive data safe and critical processes available at all times.

The ShadowtrackONE monitoring system exceeds industry standards in regards to security and is System and Organization Control (SOC) 2 Type II certified.

In addition to SOC 2, Type II compliance, ShadowtrackONE offers multiple security and/or permission levels. They can enable two-factor authentication for user sign on and offer various permission levels that include the following: Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all pertinent enrollee information), UserReadOnly (can access the database but has no control to make any changes).

SHADOWTRACKONE'S NETWORK SECURITY AND REDUNDANCY

The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the agency's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing enrollee access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

SHADOWTRACK AWS HOSTING SERVICES

Shadowtrack partners with Amazon Web Services (AWS), with servers located in different regions of the United States. Shadowtrack's activity is cloud-based, and access to their case management system or any of the raw data requires a two-factor passcode identification and authorization, along with other security measures.

SHADOWTRACK SECURITY MANAGEMENT

Shadowtrack uses an outsourced information security team consisting of a full-time dedicated Information System Security Manager (ISSM) and a full-time dedicated Information System Security Officer (ISSO) who are responsible for the management of information security throughout the organization. The team maintains security credentials, performs the technical onboarding/off-boarding work, and updates and maintains the review of the information security policies. They are responsible for enforcing the information security policies, configuring, monitoring and maintaining preventative, corrective, and detective controls within the Shadowtrack environment.

SHADOWTRACK SECURITY POLICIES

Shadowtrack has adopted the following Security Policies:

+ Access Control and Termination Policy	+ Information Security Policy
+ Asset Management Policy	+ Internal Control Policy
+ Business Continuity and Disaster Recovery Plan	+ Network Security Policy
+ Code of Conduct	+ Performance Review Policy
+ Data Management Policy	+ Physical Security Policy



- + Acceptable Use Policy
- + Change Management Policy
- + Configuration and Asset Management Policy
- + Data Classification Policy
- + Data Retention and Disposal Policy
- + Encryption and Key Management Policy
- + Risk Assessment and Treatment Policy
- + Secure Development Policy
- + Security Incident Response Plan
- + Vendor Management Policy
- + Vulnerability and Patch Management Policy

SHADOWTRACK INCIDENT MANAGEMENT

Shadowtrack's incident response procedures are detailed in its Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover Shadowtrack systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a post-mortem report. Specific steps that Shadowtrack will take are:

- + The Security Manager will manage the incident response effort.
- + All correspondence will take place within the "shadowtrack only" channel.
- + A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.

Shadowtrack will inform all necessary parties of the incident without undue delay.

SHADOWTRACK DATA BACKUP AND RECOVERY

All vital data that would be affected by disruption are maintained and controlled by the data's applicable teams. Data to be backed up include:

All data determined to be critical to company operation and/or a team member's job function.

All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.

All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

All non-ephemeral data is contained within one of two geographic regions: AWS East and West. Full backups are taken nightly. Monthly backups are taken on the first of the month. Backups are replicated between regions for geographic redundancy. Additional backup schedules and retentions terms may be configured for each of these data stores based on regulatory and contractual requirements. Backup configurations are reviewed annually to ensure compliance with this plan and the viability of recovery.

SHADOWTRACK SYSTEM ACCOUNT MANAGEMENT

Shadowtrack's access management procedures are documented in its Access Control Policy. Shadowtrack uses Role-based authorization to control access to its network infrastructure. Shadowtrack uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place that Shadowtrack uses when granting access to its systems:

- + Technical access to Shadowtrack networks must be formally documented.
- + Background checks will be performed on domestic persons granted access to Shadowtrack networks.

Only authorized Shadowtrack employees and third parties working under a signed contract or statement of work, with a business need, shall be granted access to the Shadowtrack production network.

With regards to access provisioning, Shadowtrack uses the following controls:



- + New employees and/or contractors are not to be granted access to any Shadowtrack production systems until after they have completed all HR onboarding tasks, which includes receiving and passing a background check (as applicable), review and signing of all company policies, signing of Shadowtrack's NDA, and completion of cybersecurity awareness training.
- + Access is restricted to only what is necessary to perform job duties.
- + No access may be granted earlier than the official employee start date.
- + Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system/data owner or management.
- + Records of all permission and privilege changes shall be maintained for no less than one year.
- + Access rights of users must be removed promptly within 24 hours of notification being given to the IT Manager.
- + If current access rights are no longer needed due to transfer or change of role, termination of those rights must be performed promptly within 24 hours of notification being given to the IT Manager.

SHADOWTRACK RISK ASSESSMENT

Shadowtrack's Risk Assessment process takes into account a number of factors each of which contributes to both the likelihood and potential impact of a given risk. These include:

- + The criticality of potentially impacted business processes as laid out in the Business Continuity and Disaster Recovery Policy.
- + Whether a risk could potentially impact the confidentiality, availability, integrity, or privacy of customer data, PII, or PHI.
- + Potential monetary loss.
- + The ability of the risk to impact Shadowtrack's business objectives.
- + Potential impact to Shadowtrack customers or vendors.

Shadowtrack uses Risk Treatment Plans for any response to risks other than "Accept."

SHADOWTRACK RISK ANALYSIS

In accordance with Shadowtrack's Risk Management Policy, risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where Shadowtrack chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

Mitigate: Shadowtrack may take actions or employ strategies to reduce the risk.

Accept: Shadowtrack may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.

Transfer: Shadowtrack may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Shadowtrack, or insurance may be appropriate for protection against financial loss.

SHADOWTRACK DATA COMMUNICATION

All application services accessed over public networks are required to use TLS v1.2 or above. This ensures confidentiality, integrity, and non-repudiation of the information being transmitted. Requests transmitted over insecure channels are redirected to secure channels and enforcement protocols such as HSTS are in place to enforce this requirement. Application inventory is taken monthly, and vulnerability assessment scans are conducted quarterly to ensure that these controls remain in effect for existing applications and have been put in place for any newly added applications.

Shadowtrack's Mobile applications and Web applications require secure authentication for access to data and utilize role-based access control to constrain access. Network security rules are also in place to restrict access to



servers, applications, and servers outside the scope of Web protocols. These security rules are enforced at the network and application layers and are denied by default with whitelist rules. In conjunction with the authentication and authorization built into the applications themselves, these rules prevent misrouting of online transactions and unauthorized data disclosure.

SHADOWTRACK ACCESS TO PRODUCTION CODE BASE

Shadowtrack uses HTTPS to communicate with and access its network. IP addresses have to be specifically whitelisted to allow access and implicit denial is employed. All traffic within the network is redirected from HTTP to HTTPS. Furthermore, public facing bastion servers are used to control SSH traffic to and from the network.

Access Control to the production code base is limited via the following controls:

- + The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- + RBAC approach is used for accessing the application code repository.
- + All default regular-user accounts have been removed.

SHADOWTRACK THIRD PARTY MONITORING

Shadowtrack contracts a third party to perform annual penetration tests. Shadowtrack contracts with a premier AWS tiered managed service provider to manage all the cloud servers in the AWS environment. Regarding vulnerabilities, our AWS managed service provider monitors for vulnerability issues in real-time in addition to what AWS guard duty provides.

The process for reporting of any deficiencies with regards to Shadowtrack policies and procedures is clearly spelled out in each relevant policy.

SHADOWTRACK CONTINGENCY PLAN FOR UNEXPECTED SYSTEM OUTAGES

There are many aspects of electronic monitoring systems that can experience some sort of temporary and limited outage. One example of this would be cellular communications between a cellular tower and a GPS monitoring device. These usually repair themselves very quickly. The critical issue is identifying which issues can cause a mass degradation or loss of service and preemptively architecting an approach that minimizes each. The following issues comprise a list of the items that can cause a system outage and Shadowtrack's approach to mitigation:

Wireless Network Outage. Shadowtrack's GPS devices communicate using multiple cellular network providers and automatically switch between providers and their respective roaming partners' cellular networks based on service availability. This approach ensures that if one network were to fail, be unavailable or degrade; the electronic monitoring devices would automatically fail over to other operating networks.

Core Internet Transport Failure. Core internet links fail on a periodic basis. However, the inherent architecture of the internet is self-healing. This means that there are multiple transport paths between any one location and any other location in the core network. A loss of a significant node in the internet core network would mean a slight degradation in service as opposed to a system outage.

ShadowtrackONE Software System Outage. Shadowtrack's web-based software, ShadowtrackONE is a mission critical element of the electronic monitoring system. As such, Shadowtrack has redundant instantiations of the system. If the primary software platform were to have an outage the backup platform can be engaged within minutes to prevent any prolonged system outage. This failover is periodically tested to ensure proper functionality. **Data Center Electrical or Internet Connectivity Outage.** Shadowtrack partners with Amazon Web Services (AWS), with servers located in different regions of the United States. Shadowtrack's activity is cloud-based, and access to the case management system or any of the raw data requires two-factor passcode identification and authorization along with other security measures. Operating with various locations worldwide, Shadowtrack accepts and follows



each agency's data and information record retention requirements. The systems are monitored 24/7/365; augmenting Shadowtrack's IT team in ensuring that the physical environment is both stable and secure.

Upon request, the Contractor must provide the Lead State with the results of a SOC 2 Type II covering all five (5) functional areas (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a third-party assessment based on current revision of NIST 800-53 Moderate controls conducted within the last two (2) years, or FedRAMP authorization, or GovRAMP authorization. The Lead State may terminate the Master Agreement for the Contractor's failure to provide the audit results requirements in this section within the timeframe specified in this section.

SENTINEL RESPONSE

As a leading provider of electronic monitoring programs for nearly 33 years and as the most active Contractor on NASPO ValuePoint Master Agreement #22PSX0021, Sentinel recognizes the importance of all the key elements of SOC 2 compliance. In 2022, Sentinel acquired Omnilink Systems, a division of Sierra Wireless, a publicly traded international firm who developed systems and solutions in accordance with SOC 2 specifications. As part of the acquisition, Sentinel acquired software solutions and processes that reside in the Oracle Government Cloud, a SOC 2 compliant, cloud hosted environment offering the following Best in Class security as follows.

Sentinel is undergoing our scheduled SOC 2 Engagement. This requires an independent outside firm, Clifton Larson Alan (CLA), to perform a "test of controls" to obtain evidence that the controls described by Sentinel are being implemented properly as of specific date or for the period. The type of tests used during the testing process include; inquiry, observation, inspection, and reperformance of transactions with a focus on the five (5) key elements of SOC 2 compliance which include Security, Availability, Confidentiality, Processing Integrity and Privacy.

Sentinel is prepared to provide proof of engagement and SOC 2 assessment findings upon completion and, as required, Sentinel will provide results of our third-party assessments upon request.

The Contractor must continue to maintain compliance and provide audits/assessments at least one (1) time every two (2) years throughout the term of the Master Agreement and must provide the results to the Lead State within six (6) months of completion of the audit/assessment.

SENTINEL RESPONSE

Sentinel will comply with this requirement and ensure audits/assessments are completed no less than once every two years with results provided to the Lead State within six (6) months of completion.

The Contractor must contact the Purchasing Entity immediately upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Entity's Data.

SENTINEL RESPONSE

Sentinel will immediately contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Entity's Data.

We understand the required testimony obligations, and Sentinel will provide a subject matter expert to appear in court to discuss equipment, monitoring services, etc., if required. We are fully prepared to provide qualified



personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports under oath in a court of law. Upon request of the court and/or in response to a subpoena, Sentinel will provide expert court testimony, either in person or in writing, through witnesses qualified to defend the integrity of our systems and services on behalf of the agency. We also can provide testimony via secure virtual web-based sessions, as needed, which became essential during the COVID pandemic. We can submit the monitoring documentation as supporting evidence when describing the program participant's activities while being monitored. All court testimony is supported by our Custodian of Records who will attest to the validity and accuracy of all monitoring documentation.

The Contractor must not respond to subpoenas, service of process, and other legal requests related to the Purchasing Entity without first notifying the Purchasing Entity unless prohibited by law from providing such notice.

SENTINEL RESPONSE

Sentinel will not respond to subpoenas, service of process, and other legal requests related to the Purchasing Entity without first notifying the Purchasing Entity unless prohibited by law from providing such notice.

The Purchasing Entity owns all rights, title, and interest in its Data that is related to the services provided under any Order. The Contractor must not access the Purchasing Entity's user accounts or Data, except (i) in the response to service or technical issues, (ii) as required by the express terms of the Order, or (iii) at the Purchasing Entity's written request.

SENTINEL RESPONSE

Sentinel understands and acknowledges that the Purchasing Entity owns all rights, title, and interest in its Data that is related to the services provided under any Order. Sentinel will not access the Purchasing Entity's user accounts or Data, except (i) in the response to service or technical issues, (ii) as required by the express terms of the Order, or (iii) at the Purchasing Entity's written request.

All data centers must be based in the United States.

SENTINEL RESPONSE

All data and data centers are contained within the United States.

B. Data Requirements

Each authorized user must be able to access the Contractor's software in a secure manner.

SENTINEL RESPONSE

Each authorized user is provided with their own login and once they have established their confidential password, Sentinel is able to ensure the integrity of each user's entry. This unique user access permits our Information Technology personnel to follow electronic audit trails that permit supervisors and management to verify the source of all data entries or modifications. Monitoring System Passwords are stored using salted, memory-hard hashing (Argon2id, per RFC 9106); plaintext passwords are never stored.



Access to the **SentinelDNA** Monitoring System websites, systems, privileged access, and administrative consoles is protected by multi-factor authentication. Customer access is protected by multi-factor authenticated Single Sign On. Sentinel Staff with privileged access to the system gain access over a multi-factor authenticated Client VPN. IPsec tunnels between sites are secured based on NIST SP 800-77 rev 1 specifications.

SCRAM Optix enforces role-based access controls ensuring that users access only the data and functions appropriate to their role. Multi-factor authentication is available for enhanced security.

ShadowtrackONE offers multiple security and/or permission levels. They enable two-factor authentication for user sign on and offer various permission levels that include the following: Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all pertinent participant information), UserReadOnly (can access the database but has no control to make any changes).

Data that is stored in the Contractor's software must be protected to ensure unauthorized access.

SENTINEL RESPONSE

The system is completely secure and uses state-of-the-art security measures. Login authentication is based on NIST SP 800-63-3 Digital Identity Guidelines to ensure secure access to the Monitoring System. Sentinel has employed the use of Single Sign-On (SSO) and Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.

Sentinel Staff with privileged access to the system gain access over a Multi-factor authenticated Client VPN. IPsec tunnels between sites are secured based on NIST SP 800-77 rev 1 specifications.

The Monitoring Center systems and servers use a minimum of TLS 1.2 with best practice cryptographic ciphers and modules based on FIPS 140-3 and NIST SP 800-52 Rev 2 for all HTTPS access to monitoring applications and for Data in Transit. Data at rest is encrypted using AES-256 and remains encrypted before being transmitted. If industry best practices are updated due to weaknesses being identified in any federally compliant ciphers and modules, Sentinel implements them based on severity without waiting for federal standards publications to be revised.

The system is continuously synchronized and replicated in its entirety to secondary offsite Disaster Recovery systems, in addition to all data being backed up and encrypted for off-site long-term storage.

All changes to participant or demographic information or monitoring data are saved within the system. Additionally, each employee has a specific database login credential that permits Sentinel to perform detailed audits on user access to all participant records in the database to confirm that unauthorized changes have not been made.

Our IT staff has installed all of the necessary physical and technical security measures (e.g., TLS certificates, network firewalls, Endpoint Protection providing protection from malware and ransomware, Monitoring Agents for Managed Detection and Response, access control equipment) to ensure that unauthorized users and malicious actors do not have access to Sentinel's information technology infrastructure, applications, data or our National Monitoring Center facilities.

NOTE: No participant data is stored on the hard drive of a computer accessing the monitoring system (internally or externally). In the event of the theft or destruction of a computer that has accessed our system, confidential participant data and records will not be compromised. All data is stored on our secure servers in our Primary sites in Los Angeles, California, and Oracle Cloud Ashburn, Virginia, and Disaster Recovery sites in Dallas, Texas, and Phoenix, Arizona.



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, we have taken precautions to ensure the integrity and security of our system with protection of records and their confidentiality are our primary concerns. All our security systems are monitored electronically and manually by our IT group continuously to ensure no lapse in service.

To aid in the integrity of records, Sentinel uses Intrusion Detection and Intrusion Prevention at perimeter firewalls, combined with XDR endpoint agents and MDR endpoint agents installed on every system and workstation. This data is collected into the Security Information and Events Management system operated by a 3rd party Security Operations Center that monitors the system 24x7 both manually and with automation for detected threats. Sentinel staff are immediately informed of suspicious activity on files and systems.

The proposed SCRAM CAM and Remote Breath alcohol monitoring **SCRAM Optix** platform employs a layered security architecture protected by TLS encryption for all user sessions. Role-based access controls govern data access, with authentication required for all system access. Administrative access is logged and auditable. All client data stored in SCRAM databases is encrypted at rest using industry-standard encryption, protecting against unauthorized access at the storage layer.

All information is encrypted using password protection that meets guidelines from the National Institute of Standards and Technology (NIST). SCRAM Systems web servers use SSL certificates to ensure that all session data is encrypted, and all host communications information is confidential. The entire perimeter is protected and monitored by high-availability firewalls and intrusion-detection/intrusion-prevention systems. All database data is covered by a blanket encryption software from Datrium, which is FIPS-approved AES-XTS-256 with 512-bit keys. All users must have a username and password to access the system. The application is constructed in a manner to ensure that customers do not have access to any systems operations areas and are restricted to their portal view of the data.

The **ShadowtrackONE** monitoring platform protects data transmitted between the application and supporting servers by using industry-recommended secure cipher suites to encrypt all data in transit. This includes the use of TLS 1.2 protocols and AES-256 encryption, where supported by client systems. Also, all data stored within the production environment is encrypted at rest using industry-standard 256-bit Advanced Encryption Standard (AES-256). This encryption applies to all data types, including relational databases, file storage systems, and database backups.

Contractor must have sound procedures (e.g., background checks, hiring Practices, etc.) to ensure its employees are properly authorized for access to confidential and sensitive client information. The Contractor must ensure that the confidentiality is maintained and must not disclose any such information to any third party without written authorization of the Participating Entity.

SENTINEL RESPONSE

Upon employment position needed, Sentinel's Human Resources Department posts required positions on job boards and with local Employment Development sites in the area where we will be providing contractual program services. After reviewing potential applicants, those who meet our qualifications are interviewed by telephone; if the applicant passes the telephone interview, he/she is sent an Application for Employment. After the application is received, reviewed, and approved, a face-to-face interview is arranged with the hiring manager. If the hiring manager makes an affirmative selection, an offer is made to the applicant contingent on the applicant passing a background check and drug screen. After the offer has been accepted, a background check for criminal convictions is started.

Sentinel understands the importance of hiring the best quality personnel to provide secure, confidential, and reliable service. Sentinel processes our employment candidate background checks using ADP, a company that

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



specializes in performing employment screenings. ADP performs Sentinel's screening and selection services utilizing the services of NAPBS, the National Association of Professional Background Screeners. In addition to the services provided by ADP, Sentinel performs a USIS Widescreen National Criminal/Sex Offender search, state-specific misdemeanor and felony checks based on addresses received from their personal Experian TRAC report by social security number, and five-panel drug-testing on our employees. Sentinel's review process ensures that the candidates meet all background, educational, and experience standards as set forth by contractual obligations. *We do not hire people with felony convictions or misdemeanors involving moral turpitude.*

Only authorized personnel assigned to our National Monitoring Centers or IT Group have access to program participant data, and monitoring center personnel are unable to modify or alter monitoring data. Monitoring data is electronically impervious to modification or manipulation. At no time will we ever disclose confidential data to any unauthorized personnel without written approval of the participating agency or by an officer providing a confidential verbal password. All program data is maintained in accordance with industry-accepted secure data protection standards. The only staff members who are authorized to access or receive information on program participants are those who have undergone a background check and are assigned to support 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 assigned to the monitoring center and IT Group is required to undergo a thorough background check (including drug testing) and sign a Confidentiality or CORI (Criminal Offender Record Information) form when hired; any violation of these requirements will result in the termination of the employee's employment. All records created for participants referred to this program will remain the property of the participating agency and will not be released without the written consent of the agency or due to compliance with a legal subpoena. Upon completion of services, all records are returned to the participating agency or destroyed under direction of agency-authorized personnel.

Further, upon hiring, all our employees are provided with an employee handbook that outlines Sentinel's "zero tolerance" policy regarding compromising relationships with participants, their families and customer staff. We will report any conflicts of interest, improprieties, or the appearance thereof, immediately to the operational management contact of the participating agency.

The Contractor must be able to create user groups with varying access privileges (e.g., read/write and read only).

SENTINEL RESPONSE

Sentinel's DNA Monitoring Application offers hierarchy user levels that will allow the system administrator the ability to limit the tasks available to a particular user and/or group of users through role-based access controls. DNA will enable the designated system administrator to set access levels for each authorized user. Additionally, the system administrator will have the ability to establish access levels to specific caseloads or groups in any combination for authorized users. The system administrator will have the ability to secure and restrict, or alternately enable, access to clients and their information including the ability to set varying access privileges such as read/write and read only.

The **SCRAM Optix** platform enforces role-based access controls ensuring that users access only the data and functions appropriate to their role. Multi-factor authentication is available for enhanced security. The system has the ability to restrict, or enable access to, clients and their information, including the ability to set varying access privileges.

ShadowtrackONE offers multiple security and/or permission levels. They can enable two-factor authentication for user sign on and offer various permission levels that include the following: Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all



pertinent participant information), UserReadOnly (can access the database but has no control to make any changes).

Each Client's location data must be accessible for a minimum of seven years (or as designated by Participating Entity). Before it is archived or stored offline.

SENTINEL RESPONSE

Sentinel will make all participant data available as contractually agreed and has the capability of making data available for any length of time required. Sentinel will ensure data is available for a minimum of seven years or as designated by the Participating Entity.

Archived copies of each participant's location data must be retained for a minimum of seven years (or as designated by Participating Entity) and/or provided in a format that can be stored and easily interpreted by the Participating Entity.

SENTINEL RESPONSE

Sentinel will ensure archived data of each participant's location is retained for a minimum of seven years or as designated by the Participating Entity. Sentinel will provide needed exports in the format contractually agreed.

The Contractor must backup the system data at least every 24 hours.

SENTINEL RESPONSE

Sentinel backs up our monitoring system data at least every 24 hours. Sentinel hosts DNA on a VMware vSphere cluster with redundant servers, networking, and storage and maintains separate plans for System Restores from Backup and for Disaster Recovery.

Sentinel uses Zerto for VMware to continuously sync the Los Angeles DNA product system to the Disaster Recovery in Dallas Texas that is currently maintaining a 10-second RPO and 26-minute RTO based on the most recent annual failover test from November 21, 2025.

Sentinel uses Veeam for vSphere to regularly backup Database and Application servers. DNA Server VMs are backed up on the following schedule: monthly full backups, daily incremental backups, and weekly synthetic full backups which are a compilation of the last week of daily incremental backups. Transaction logs of Databases are created every 15 minutes. File server changes are backed up every 15 minutes. All backups are encrypted before being stored on disk locally. Backups remain encrypted before being transmitted offsite to Amazon S3 for long term storage. The latest full backup is kept locally for faster restores. Backup job health checks are run monthly. Restores from Backup have not been needed in over 5 years, so IT Operations annually tests at least 1 major Database VM from backups as a further health check of operational confidence.

Only IT Operations employees have access to the Veeam and Zerto backup systems. All backups, access, and changes are audited. Only IT Operations employees have access to backup encryption keys.

Veeam and Zerto send notifications to IT Operations for any backup problems. IT Operations also uses Zabbix to monitor key statuses of both Veeam and Zerto.

Veeam and Zerto servers run Sentinel's Endpoint and MDR protection agents with additional logging for access and security.



Zerto Virtual Replication Appliances (VRA) network traffic is captured by the MDR provider's on-prem network packet analyzer. Traffic from the VRAs is also logged at the perimeter firewall providing further audit logging of activity outbound or across the IPsec tunnels to the Disaster Recovery site. All network packet analysis and firewall logs are ingested into the 3rd Party MDR provider's SIEM.

SCRAM Systems replicate all data daily to online storage arrays at multiple geographic locations to ensure the availability of all data. The database is tested weekly to ensure system backup can be used for recovery of any system. In addition, SCRAM Systems completes a data "snapshot" every four hours to maintain backups. Transaction logs for all activities ensure that a data restore will be complete and that each transaction is available. A full mirror of the database is maintained, which is approximately 20 seconds behind the production database with full replication and data journaling in a near real-time mode.

Shadowtrack conducts backups of the database on a 24-hour daily basis.

Data generated as a result of the location monitoring must be owned by the Participating Entity and may not be used in any way by the Contractor without consent of the Participating Entity. The Contractor must ensure that all data is available to the Participating Entity in the event the contract is terminated, or the Contractor goes out of business.

SENTINEL RESPONSE

Sentinel understands and acknowledges that data generated as a result of the location monitoring will be owned by the Participating Entity and will not be used in any way by Sentinel without consent of the Participating Entity. Sentinel will ensure that all data is available to the Participating Entity in the event the contract is terminated, or Sentinel goes out of business.

II. RESPONSE TO TECHNICAL CRITERIA

II. RESPONSE TO TECHNICAL CRITERIA

SECTIONS A, B, AND C SHOULD BE COMPLETED ACCORDING TO THE CATEGORY(IES) TO WHICH YOU ARE RESPONDING:

SENTINEL RESPONSE

The subsequent pages contain narrative overviews of Sentinel's technologies, services, and options available for utilization in an electronic monitoring services program. 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 traditional radio frequency monitoring or mobile app check-in, as well as higher risk participants who are monitored through global positioning satellite tracking. We also provide solutions such as state-of-the-art alcohol monitoring, including both portable breath testing as well as transdermal continuous 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 a Participating Entity. Additionally, all our monitoring services proposed herein are performed directly through our own monitoring center, which is operational 24 hours a day, seven (7) days a week, 365 days a year.

—IMPORTANT SENTINEL ADVANTAGE—

As one of the nation's leading providers of electronic monitoring/offender services, with twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement #22PSX0021, Sentinel has



unparalleled experience in electronic monitoring and more specifically in successfully marketing national NASPO cooperative contracts. Additionally, for NASPO RFP #22PSX0021, Sentinel is a NASPO ValuePoint contractor in all three (3) technology categories:

- + Category 1: Radio Frequency Monitoring
- + Category 2: Alcohol Monitoring
- + Category 3: GPS Satellite Monitoring
- + Each category additionally encompassing Optional Contractor Provided Services

As a longer-term partner to NASPO, Sentinel has truly demonstrated and proven to serve as “a one-stop shop.” We stand ready to continue providing services for the new Electronic Monitoring contract with technology and services to meet all categories required.

A. SCOPE OF WORK – CATEGORY 1: GPS

A. Scope of Work – Category 1: GPS (offerors are required to answer all questions if proposing for GPS Services)

1. Describe your plan for meeting the Master Agreement Objectives identified in Attachment 02, Scope of Work.

SENTINEL RESPONSE

Below, Sentinel has provided our plan for meeting the Master Agreement Objectives for **Category 1: GPS Monitoring**, including an ankle-worn solution and an optional wrist-worn GPS solution along, identified in **Attachment 02, Scope of Work**.

A. GPS Hardware

IV. Category 1: GPS Monitoring. To include ankle-worn and wrist-worn GPS solutions.

A. Hardware Requirements:

SENTINEL RESPONSE

OM500

Sentinel is proposing the most advanced member of the OM Series one-piece GPS device family, the OM500™ GPS tracking unit, which is both the transmitter and receiver of information in one unit. The OM500 is equipped with onboard processing capabilities and communicates with the host system via the Verizon or the AT&T LTE network. This multi-carrier functionality provides a benefit to the Participating Entity because, based on any geographic limitations of cellular/communication coverage in remote areas, authorized staff can use the preferred carrier for that region. Prior to program transition, Sentinel will work closely with Participating Entity staff to determine which communication carrier works best in that region, thereby ensuring optimal service provision.



The unit allows for customized tracking and reporting intervals to be assigned at the client level and can store more than ten (10) days of tracking information in the onboard non-volatile memory, regardless of the mode of operation, should the unit be unable to communicate with the web-based system. The OM500 is also able to store zones on board the device to provide real-time tracking and immediate notifications on zone alerts. In addition, based on its performance capabilities, the OM500 does not require the use of a home unit or beacon to monitor participants 24/7. Through the use of three (3) state-of-the-art tracking and location technologies, including GPS,



Wi-Fi, and Cellular Services, a geographic Home Zone can be used to ensure the participant's compliance with curfew or stay at home restrictions are accurately monitored.

SHADOWATCH (OPTIONAL)

We are also proposing as **an option** for Participating Entities that require a wrist worn device, the ShadoWatch™, which is a wrist-worn GPS device for monitoring and supervising low to moderate risk clients, and/or clients with medical conditions that prevent the use of an ankle monitoring device assigned to electronic monitoring. The ShadoWatch is a discreet wrist-worn one-piece GPS tracking device that helps properly monitor low risk program participants compliance.

ShadoWatch is designed specifically for offender tracking and carries the IP68 international waterproof, dust, and debris certification. It can withstand submersion in water up to 3 meters for 30 minutes. The ShadoWatch is shock resistant and tamper-proof, with titanium reinforcement within the strap, as well as heart rate and motion sensors to further detect noncompliance.

The ShadoWatch provides ample battery power and staff can be alerted if there are any Low Battery conditions that occur. The unit offers 24+ hours of battery life while providing 1-minute location intervals and 70+ hours of battery life while providing 5-minute location intervals. However, when using the remote charger (as detailed below in the specification response section) the ShadoWatch will continue to function as designed and provide more than 70 hours of optional battery life. The battery requires a charging period of 90 – 120 minutes. The ShadoWatch is equipped with a wireless charger that simply snaps onto the watch allowing the participant to freely move around while charging. The wireless charging block simply attaches to the ShadoWatch to initiate device charging and extends the daily operation battery life.



- The tracking device must use easy-to-install straps that ~~are~~ should be re-usable, adjustable, and require no cutting or specially designed tools by the agency to fit on a client. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

OM500

The OM500 tracking device is easily installed by the trained Participating Entity officer in under five (5) minutes without cutting or specially designed tools. The OM500 GPS tracking device is shipped to the Participating Entity's location with the standard, reusable, adjustable strap already connected and is immediately ready for easy installation without the use of any tools. The OM500 is extremely easy to attach to the participant's ankle with a heavy-duty reusable, adjustable and replaceable strap. The strap is designed and has been in use for over 10 years to provide a comfortable and secure fit with multiple sizing options to ensure the proper fit on each person. Two (2) locking pins connect the unit to the back plate. Once properly attached to the ankle, the device will immediately detect and report a tamper message if it is removed. The OM500 GPS tracking device strap is easily sanitized and reusable on multiple participants without the need for replacement. The standard sized strap fits 99% of the population and an extended length strap is available to accommodate the largest ankles. An optional cut-resistant strap is also available as an alternative to the OM500 standard strap.

SHADOWATCH (OPTIONAL)

The installation process for the wrist-worn ShadoWatch is quite simple and takes only minutes to install. The device should be assigned to the participant in the monitoring database and the battery should be fully charged prior to installation. To begin the installation process, one side of the strap is locked onto the device housing by



attaching it with two (2) screws. The strap is then sized by placing the ShadoWatch and strap around the participant's wrist. One finger width should be between the strap and the participant's skin. Once the proper size is determined, the excess strap is removed and the device is installed by inserting the two (2) remaining screws into the open end of the strap and the device housing. Once the device is locked in place on the participant's wrist, security covers are then snapped in place to cover the screws on each side of the device housing.

- All equipment and systems furnished must be standard products of the manufacturer identified, must be in proper working order and clean and free from defects of features affecting appearance or serviceability, or the safety of the client in normal intended use.

SENTINEL RESPONSE

OM500

Sentinel is the Original Equipment Manufacturer (OEM) of the proposed OM500 one-piece ankle-worn Global Positioning Satellite (GPS) tracking solution, and all equipment and systems furnished will be Sentinel's standard products in working order and clean and free from defects or features affecting the appearance, serviceability, or safety of the client while in normal intended use.

SHADOWWATCH (OPTIONAL)

Shadowtrack Technologies is the Original Equipment Manufacturer (OEM) of the proposed ShadoWatch one-piece wrist-worn Global Positioning Satellite (GPS) tracking solution, and all equipment and systems furnished will be Sentinel's standard products in working order and clean and free from defects or features affecting the appearance, serviceability, or safety of the client while in normal intended use.

- Must be capable of communicating with the Contractor's software and detect the following events and communicate to Contractor's web-based platform, and app via a tablet or mobile device:
 - Arrival and departure from inclusion and exclusion zones as defined by Participating Entity
 - Unauthorized arrival or departure as defined by Participating Entity
 - Battery low alerts
 - Strap and/or device tamper alerts
 - Tracking device failed to call in alerts
 - Efforts to tamper with the tracking device
 - Loss of location
 - Potential cellular jamming
 - Communication Loss

SENTINEL RESPONSE

OM500

The OM500 tracking device will detect the following events and communicate with the Sentinel web-based monitoring system:



- + **Arrival and departure from inclusion and exclusion zones as defined by Participating Entity:** The OM500 will report all arrivals and departures from inclusion and exclusion zones as defined by the Participating Entity. Each exit from, and entry to, the residence or zone (inclusion or exclusion) is reported by the GPS unit, and the DNA web-based system automatically compares the activity's location with the set zones and participant schedule when reporting the event.
- + **Unauthorized arrival or departure as defined by Participating Entity:** Any discrepancies of the event time or location with the permitted time or location, as defined by the Participating Entity, will generate a violation that is processed by DNA.
- + **Battery low alerts:** The OM500 will provide low battery and dead battery alerts to the Participating Entity. Additionally, the Participating Entity can establish low battery settings and alerts for program participants. The OM500 will also automatically notify the participant of a low battery situation with a voice command instructing the participant to charge the device.
- + **Strap and/or device tamper alerts:** The OM500 unit is equipment with both strap and device tamper alerts. The OM500 has multiple tamper detection features to ensure the OM500 is not removed without detection. The water and light sensors inside the case protect the device by generating an alert when triggered. The device is connected to a reusable backplate that has two (2) pressure switches that detect any removal attempts. The strap is attached to the back of the device which limits possible false tampers and requires no tools for installation. Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment.
- + **Tracking device failed to call in alerts:** Should the OM500 device be unable to "call in" or communicate with the monitoring system, the device will continue to track and store location and event information in its robust, non-volatile onboard memory, regardless of the mode of operation. The OM500 unit will transmit the stored data to the monitoring system as soon as communication is restored; all alerts will be specified, in historical order, and responded to appropriately. Sentinel's DNA monitoring system will continue to alert Participating Entities of the failed call-ins as instructed in the Entity's notification protocols.
- + **Efforts to tamper with the tracking device:** The OM500 is equipped with triple tamper detection including 1) fiber-optic strap design tamper, 2) device case tamper, and 3) backplate tamper. Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and dual pressure sensors within the device, the OM500 device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tampers with the strap. The OM500 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate, indicative that the device has been uninstalled/disassembled. Additionally, the unit will send a tamper alert if the unit is broken/cracked or if the unit's backplate is separated from the rest of the device.
- + **Enhanced detection and reporting of device Potential Slippage:** In addition to the OM500's three (3) tamper types already developed and implemented, Sentinel has developed an even more robust approach to detect and report possible unidentified removal via the Potential Slippage alert. Within our internal firmware, Sentinel is maximizing the benefits of the OM500 internal components. By utilizing the accelerometer in combination with cellular signal measurement, "Tilt" measurements, Wi-Fi changes and GPS signal strength, we have developed an even more advanced tamper/removal detection solution to accompany our original leading edge tamper technology.
- + **Loss of location:** In the event the OM500 were to lose location, the OM500 is equipped with three (3) location technologies - GPS, Cellular, and Wi-Fi technologies - to ensure that program participants are continually tracked, even in the absence of satellite signals. This triple-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the OM500 will automatically switch to cellular tracking and Wi-Fi technologies to continue tracking the participant. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The unit will continue to track and store location data and will transmit the stored location data upon restoration of location



services. Sentinel's DNA monitoring system will continue to alert Participating Entities of the loss of location as instructed in the Entity's notification protocols.

- + **Potential Cellular Jamming:** The potential jamming or shielding of the OM500 is detected based on various parameters/characteristics of GPS, Cellular and Wi-Fi signals. The system analyzes the RF noise characteristics and levels along with knowledge of signals that are not present to identify if the lack of signal is due to the environment or due to potential shielding/jamming of the unit. Unchanged cellular, and Wi-Fi coupled with location change generate an alert that is captured and reported within the SentinelDNA monitoring system.
- + **Communication Loss:** In the event the OM500 cannot communicate with the monitoring system, the OM500 is capable of indefinitely storing more than ten (10) days of tracking information in its robust, non-volatile onboard memory, regardless of the mode of operation, should the unit be unable to communicate with the web-based system. The OM500 unit will transmit the stored data to the monitoring system as soon as communication is restored; all alerts will be specified, in historical order, and responded to appropriately. Sentinel's DNA monitoring system will continue to alert Participating Entities of the communication loss as instructed in the Entity's notification protocols.

Additionally, officers will be able to view these events through SentinelDNA and the DNA Mobile App via any internet-enabled device, including desktops, laptops, tablets, and smartphones.

SHADOWATCH (OPTIONAL)

The optional ShadoWatch wrist worn GPS tracking device will detect the following events and communicate with the Sentinel web-based monitoring system:

- + **Arrival and departure from inclusion and exclusion zones as defined by Participating Entity:** The ShadoWatch will report all arrivals and departures from inclusion and exclusion zones as defined by the Participating Entity. Each exit from, and entry to, the residence or zone (inclusion or exclusion) is reported by the GPS device, and the Shadowtrack web-based system automatically compares the activity's location with the set zones and participant schedule when reporting the event.
- + **Unauthorized arrival or departure as defined by Participating Entity:** Any discrepancies of the event time or location with the permitted time or location, as defined by the Participating Entity, will generate a violation that is processed by the ShadowtrackONE monitoring application.
- + **Battery low alerts:** The ShadoWatch will provide low battery and dead battery alerts to the Participating Entity. Additionally, the Participating Entity can establish low battery settings and alerts for program participants. The ShadoWatch will also automatically notify the participant of a low battery situation.
- + **Strap and/or device tamper alerts:** The ShadoWatch device is equipped with both strap and device tamper alerts. The ShadoWatch has multiple tamper detection features to ensure the ShadoWatch is not removed without detection. The ShadoWatch is shock resistant and tamper-proof, with reinforced strap. Additionally, if they attempt to remove the device by trying to slip it off their wrist, a Proximity Tamper will alert them to the unauthorized removal and supervising personnel will be immediately notified.
- + **Tracking device failed to call in alerts:** Should the ShadoWatch be unable to "call in" or communicate with the monitoring system, the device will continue to track and store location and event information in its robust, non-volatile onboard memory, regardless of the mode of operation. The ShadoWatch unit will transmit the stored data to the monitoring system as soon as communication is restored; all alerts will be specified, in historical order, and responded to appropriately. Any compliance deviations can be immediately reported to supervising staff and notifications can be immediately generated by Shadowtrack's automated monitoring system.
- + **Efforts to tamper with the tracking device:** The ShadoWatch is equipped with triple tamper detection including 1) fiber-optic strap design tamper, 2) device case tamper, and 3) proximity tamper. Within seconds the ShadoWatch generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and proximity sensors, the ShadoWatch device automatically and instantly communicates to the monitoring system when a participant attempts to



remove the device or tamper with the strap. The ShadoWatch device will send a tamper alert if the participant severs the strap or if they attempt to slip the device off their wrist by generating a Proximity Tamper.

- + **Enhanced detection and reporting of device Potential Slippage:** If the participant attempts to remove the ShadoWatch device from their wrist by cutting it off, a Band Tamper Alarm will generate or if they attempt to remove the device by trying to slip it off their wrist, a Proximity Tamper will alert to the unauthorized removal and supervising personnel will be immediately notified. The device can be set to various tracking intervals based upon the user agency's desired preference and location data will be reported to our monitoring platform.
- + **Loss of location:** In the event the ShadoWatch were to lose location, the ShadoWatch is equipped with three (3) location technologies - GPS, Wi-Fi technologies, and Cellular, to ensure that program participants are continually tracked, even in the absence of satellite signals. This triple-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the Wi-Fi technologies will automatically switch to Wi-Fi location, and cellular based technologies to continue tracking the participant. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The unit will continue to track and store location data and will transmit the stored location data upon restoration of location services. The ShadowtrackONE monitoring system will continue to alert Participating Entities of the loss of location as instructed in the Entity's notification protocols.
- + **Potential Cellular Jamming:** The ShadoWatch can detect No Locations and can Escalate No Location events in accordance with the Participant Entities Notification Protocols. Further, under these types of reported events, alerts can be set up in the ShadowtrackONE monitoring application to notify the agency.
- + **Communication Loss:** ShadoWatch devices communicate using multiple cellular network providers and automatically switch between providers and their respective roaming partners' cellular networks based on service availability. This approach ensures that if one network was to fail, be unavailable or degrade; our electronic monitoring devices would automatically fail over to other operating networks. In the event the ShadoWatch cannot communicate with the monitoring system, the ShadoWatch is equipped with Onboard Memory capable of storing up to 52 days of locations in case of unavailable network upload. The ShadoWatch device will transmit the stored data to the monitoring system as soon as communication is restored; all alerts will be specified, in historical order, and responded appropriately. The ShadowtrackONE monitoring system will continue to alert Participating Entities of the communication loss as instructed in the Entity's notification protocols.

Additionally, officers will be able to view these events through ShadowtrackONE monitoring application and the Shadowtrack Mobile App via any internet-enabled device, including desktops, laptops, tablets, and smartphones.

- Must have optional grace period for early leave and late returns.

SENTINEL RESPONSE

OM500

Sentinel's monitoring platform allows the Participating Entity to set a grace period associated with zones and scheduling. This grace period allows the agency to establish a length of time that the device can be out of range before recording a violation. The grace period is adjustable and determined by the needs of the agency. The grace period can be as little as one (1) minute, or it can be set to upwards of 60 minutes; the length of the grace is completely controlled by the agency.



SHADOWATCH (OPTIONAL)

The ShadowtrackONE monitoring application includes the capability to customize grace periods for early leaves and late returns. By incorporating grace periods. If an agency elects to use grace periods, this will give the program participants the ability to leave early or return late within the pre-set grace period without the need for the agency staff being alerted, thus increasing time and efficiency for the agency staff. All actual leave and return times will be posted in the monitoring application.

- The tracking device must have the ability to fully activate indoors without the need to acquire GPS.

SENTINEL RESPONSE

OM500

The OM500 is equipped with three (3) location technologies to ensure that program participants are continually tracked, even in the absence of satellite signals. **The OM500 uses GPS, Cellular, and Wi-Fi technologies to track program participants' locations.** This **triple-tracking technology** provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the OM500 will automatically switch to cellular tracking and Wi-Fi technologies to continue tracking the participant. Wi-Fi location points are generated using precision location services from Skyhook and the OM500 device will switch to Wi-Fi points when the device is unable to obtain GPS points. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The combination of these advanced location technologies allows for the quickest acquisition time and the ability to fully activate the device indoors without being required to go outside to acquire a GPS signal.

SHADOWATCH (OPTIONAL)

The ShadoWatch is equipped with multiple location technologies. Tracking data is achieved through the ability of the device to obtain its location through GPS Satellite data and Wi-Fi data, as well as Location Based Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the devices are in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS nor Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located.

- The tracking device must have a method of ensuring accuracy of location points.

SENTINEL RESPONSE

OM500

The OM500 is a continuous Global Positioning System (GPS) electronic monitoring solution that provides near-real-time reporting of individual locations within a range of plus or minus 30 meters. The OM500 collects GPS location data once per minute and leverages GPS, Cellular, and Wi-Fi technologies to track program participants' locations for always-on, high-precision tracking. The OM500 GPS tracking device communicates with the Global Navigation Satellite Systems (GNSS) Constellation of Satellites, including GPS, Galileo, GLONASS, and BeiDou satellite constellations and provides accurate GPS location points to within approximately 10 meters outdoors and approximately 30 meters indoors.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

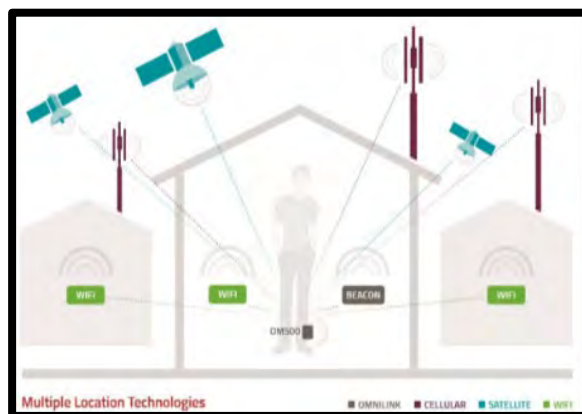


Sentinel's OM500 incorporates multiple advanced technologies specifically designed to deliver a high degree of accuracy that automatically measures, calculates, and reflects any accuracy deviation in a number of feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby increasing officer confidence.

- + **Industry Leading Triple Tracking Capability via GPS, Wi-Fi location Points, and Cellular Tracking.** In impaired areas where GPS cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. This allows for a significantly more robust device as it offers multiple communication options.
- + **On-Screen Accuracy Precision reading for every Tracking Point.** The Sentinel DNA web-enabled monitoring and case management software automatically maximizes the accuracy of the multiple location technologies (GPS, Cellular, or Wi-Fi) into one/the same tracking point, generating one of the most accurate points available. Tracking points are differentiated by color according to the type of point, and each point is numbered in order of occurrence. For any tracking point the user hovers their mouse pointer over, Sentinel DNA automatically provides a "Precision" feature that measures, calculates, and reflects any accuracy deviation in a number of feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby significantly increasing officer confidence.

Sentinel's proposed OM500 GPS tracking device and DNA web-based monitoring system are equipped with technology that automatically measures and reports accuracy and identifies any potential drift and ensures that participant's points on the map are accurate. Sentinel's GPS tracking solution can determine the participant's location to within better than 30 feet.

The OM500 is equipped with multiple location technologies to ensure that program participants are continually tracked by the OM500 device in the absence of cellular communication networks. The OM500 uses GPS, cellular and Wi-Fi technologies to track program participants' locations. This multi-faceted tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the OM500 will switch to cellular and Wi-Fi technologies to continue tracking the participant. Wi-Fi location points are generated using precision location services from Skyhook, and the OM500 device will switch to Wi-Fi points when the device is unable to obtain two or more consecutive GPS points. The OM500 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM500's unique design combines multiple layers of location technologies including cellular and Wi-Fi whereby the device does not have to connect to the Wi-Fi signal, and the signal only needs to be visible to the device. Also, the Wi-Fi location points are generated on the impaired part of the rate plan. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The combination of these advanced location technologies allows for the quickest acquisition time (typically within 60 seconds, so long as there is a cellular signal detected) without being required to go outside to acquire a GPS signal when enrolling and installing a device.



The Sentinel DNA web-enabled monitoring and case management system automatically maximizes the accuracy of the multiple location technologies (GPS, Cellular and/or Wi-Fi) into one of the most accurate points available. Tracking points are differentiated by color according to the type of point (Satellite-based, combination of Satellite and Cell Tower based, Wi-Fi based), and each point is numbered in order of occurrence. Additionally, by hovering

Request for Proposals for
ELECTRONIC MONITORING

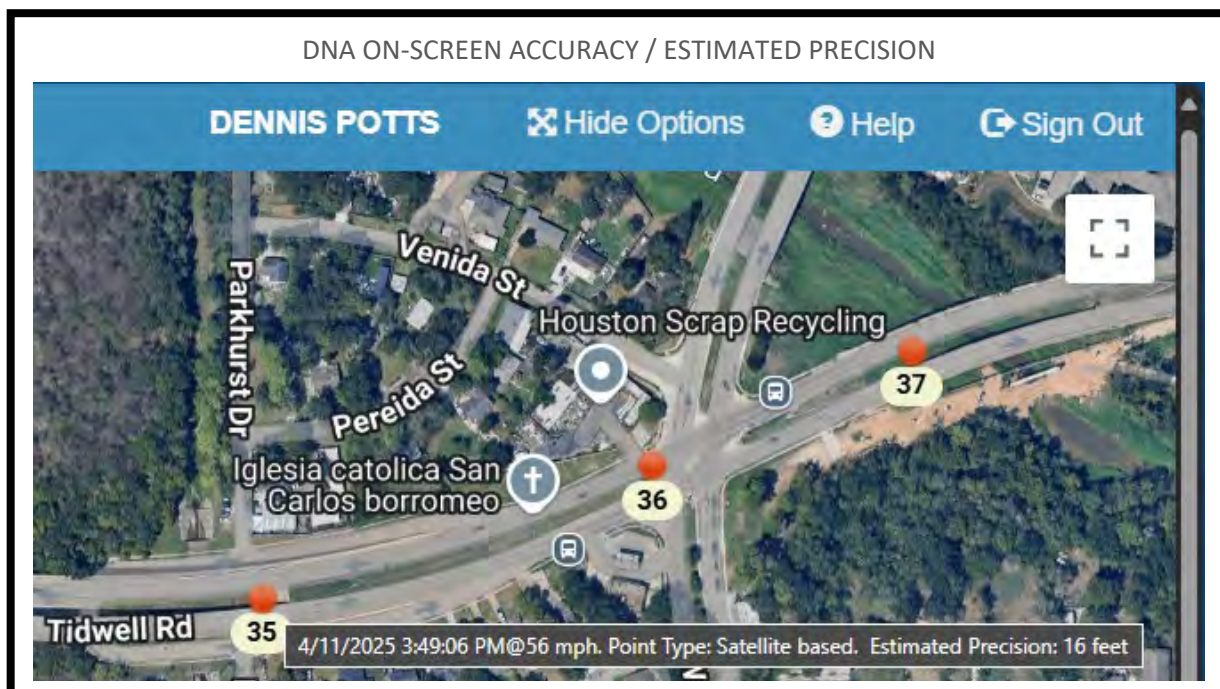
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



over any point on the location history screen, the DNA monitoring application system will display the date and time of the location point, the speed of the point, the type of point that was acquired, and the Estimated Precision or Accuracy of the point.

—IMPORTANT SENTINEL ADVANTAGE—

As an added DNA feature, when a user hovers the mouse pointer over any tracking point an embedded on-screen rollover window appears showing the date, time, speed and estimated precision (onscreen accuracy) of the tracking point. The screen below displays a participant's location history with an on-screen accuracy of "Estimated Precision: 16 feet" This advanced feature provides an instant added confidence to officers regarding the relative accuracy of any tracking points of interest. Also, the second screen shot shows accurate tracking in an underground subway system in Washington, DC with a high rate of accuracy and in real-time.

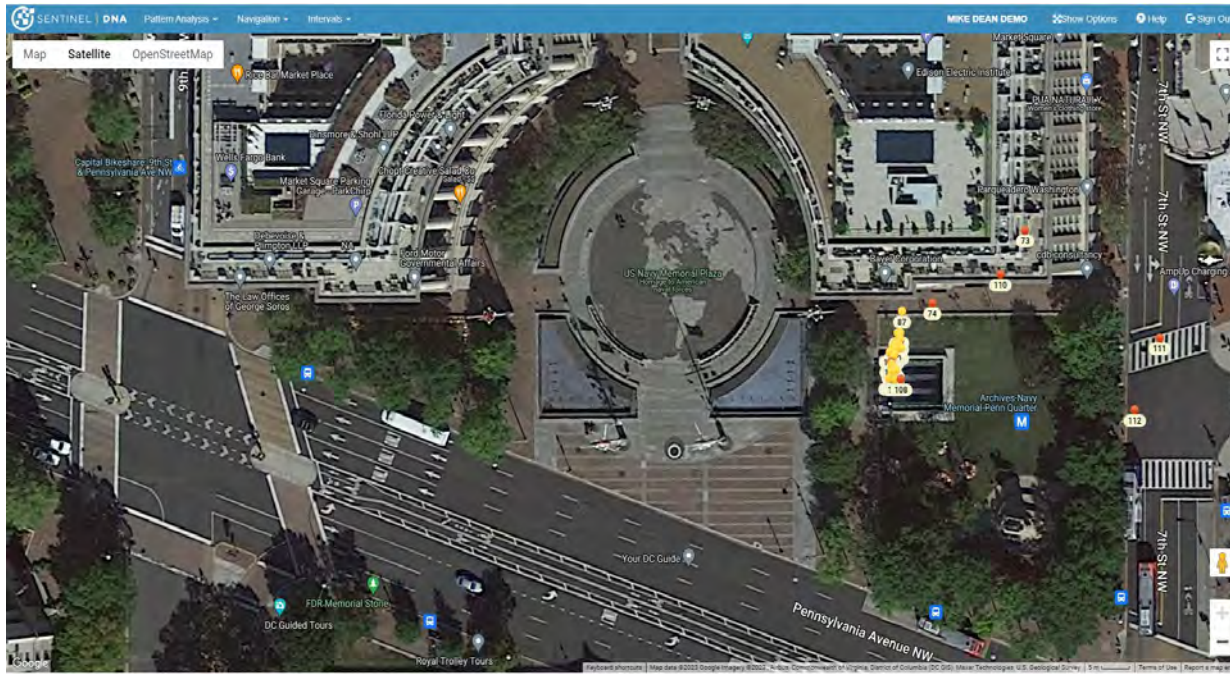


Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



ABILITY TO TRACK LOCATION IN AN UNDERGROUND SUBWAY SYSTEM IN REAL TIME
AND ACCURATE PROVIDE LOCATION POINTS VIA Wi-Fi





SHADOWWATCH (OPTIONAL)

ShadoWatch includes the most up-to-date tracking options designed for the utmost accuracy and redundancy including not only GPS capabilities, but also Wi-Fi and Location Based Service (LBS) tracking redundancies.

The ShadoWatch wrist worn GPS device is a continuous Global Positioning System (GPS) electronic monitoring solution that provides near-real-time reporting of individual locations within a range of plus or minus 10 meters outdoors and plus or minus 30 meters indoors. The ShadoWatch collects GPS location data once per minute and leverages GPS, Cellular, and Wi-Fi technologies to track program participants' locations for always-on, high-precision tracking. The ShadoWatch is designed to search for and utilize satellites from various global positioning systems, including GPS, BDS, GLONASS, and others. It automatically selects satellites with the strongest signals to ensure optimal performance. This advanced technology allows the watch to use more than three satellites simultaneously for accurate and reliable tracking. The ShadoWatch incorporates multiple advanced technologies specifically designed to deliver a high degree of accuracy that automatically measures, calculates, and reflects any accuracy deviation in several feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby increasing officer confidence.

ShadoWatchTracking Method & Priority

The criteria for switching between GPS, WiFi, and LBS points on the watch are based on the availability of GPS data within each packet through the:

1. **Simultaneous Acquisition:** The watch attempts to obtain both GPS and WiFi data within each packet.
2. **Preference for GPS:** If GPS data is available in the packet, it is given priority and used over WiFi data.
3. **Fallback to WiFi:** If no GPS data is obtained in the packet, the watch will use the available WiFi data.
4. **Fallback to LBS if no GPS or WiFi:** The watch will then attempt to plot an LBS point.
5. **No Direct Switching to WiFi:** The watch does not switch from GPS to WiFi directly. Instead, it continuously tries to get both types of data in each packet and prioritizes GPS

By following this approach, the watch ensures the most accurate location data is used, leveraging GPS when possible and falling back to WiFi only when GPS is unavailable.

Sentinel is offering an optional ShadowBeacon that is designed for indoor tracking and acts like a traditional Radio Frequency (RF) device to always provide continuous monitoring. Often used in areas of impaired GPS signals such as inside large warehouse facilities or used to more tightly define/restrict a program participant's movement in smaller areas such as high-rise apartment buildings. The ShadowBeacon has three programmable range settings to adjust to specific areas and can be paired with ShadoWatch. Features of the optional beacon include:

- + Small design
- + Tamper-proof – detects if ShadowBeacon is moved
- + Mounts with adhesive strips to walls/ceilings
- + Completely self-contained – requires no AC power or telephone connectivity
- + Adjustable range settings





- The tracking device must communicate over a Global System for Mobile Communications (GSM) or 4G/LTE (or better) networks.

SENTINEL RESPONSE

OM500

Sentinel's proposed GPS equipment utilizes reliable and robust cellular coverage for reporting and communications. The OM500 units are available on either the Verizon or AT&T 4G LTE cellular data networks that provide robust coverage throughout the United States and the US Territories as well as Canada.

SHADOWATCH (OPTIONAL)

ShadoWatch operates on the latest 4G and 5G cellular networks and offers the most comprehensive cellular communications coverage for offender GPS monitoring programs. In addition, ShadoWatch has the ability to operate on multiple cellular carrier providers in order to offer the most comprehensive cellular coverage and to ensure that monitoring points and data are received on a continuous basis.

- Tracking device must be water resistant, durable, and able to withstand vibrations from normal client use over time.

SENTINEL RESPONSE

OM500

The OM500 units are shock resistant, water resistant, unaffected by normal human environmental and atmospheric conditions, and do not pose a safety or health threat to the wearer or unduly restrict the activities of the participant. The OM500 is capable of enduring shock and vibration associated with normal wear and use. The unit can withstand temperatures between -4° Fahrenheit and 140° Fahrenheit, humidity of more than 95 percent, normal household and atmospheric conditions, and up to 500 MHz of random vibration of 1.25G rms. The OM500 is IP67 certified and IP68-compliant. The casing and strap are both made of hypoallergenic materials and contoured to the ankle to reduce any discomfort in wear to the participant. There are no metal parts that may cause injury to either the field officer or client.

SHADOWATCH (OPTIONAL)

ShadoWatch is designed specifically for offender monitoring and carries the IP68 international waterproof, dust, and debris certification. It can withstand submersion in water up to three (3) meters for 30 minutes. Further, the ShadoWatch is capable of enduring shock and vibration associated with normal wear and use. The unit can withstand operational temperature between -20°C to +60°C. The casing and strap are both made of hypoallergenic materials and contoured to the wrist to reduce any discomfort in wear to the participant. There are no metal parts that may cause injury to either the field officer or client.

- The Contractor must offer a GPS tracking device with a reusable strap and/or a disposable strap as determined by the Purchasing Entity.

SENTINEL RESPONSE

OM500

The OM500 device is extremely easy to attach to the participant's ankle with a reusable, adjustable and replaceable strap or a disposable strap, as determined by the Purchasing Entity. The OM500 GPS tracking device



reusable strap is easily sanitized and reusable on multiple participants without the need for cutting or replacement. The reusable strap meets National Institute of Justice NIJ Standard 1004 for Offender Monitoring, is hypoallergenic, and is made of Thermoplastic Polyurethane, with a Shore hardness of approximately 45D, and is embedded with fiberoptic lines that detect strap cuts and stretching. The device is attached to the participant's ankle with an extended length band to accommodate the largest ankles. The strap's design allows for a secure fit and has multiple holes to assist in finding the proper fit on each person without the need to cut or replace. 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. Straps are designed for 24 months of service and commonly proactively replaced at a 12-to-18-month interval.

SHADOWATCH (OPTIONAL)

The ShadoWatch wrist worn GPS device is extremely easy to attach to the participant's wrist with a reusable, adjustable and replaceable strap or a disposable strap, as determined by the Purchasing Entity.

- Tracking device must not require tools for installation.

SENTINEL RESPONSE

OM500

The OM500 tracking device does not require tool for installation. As stated above, the OM500 tracking device is easily installed by the trained Participating Entity officer in under five (5) minutes without cutting or specially designed tools. The OM500 GPS tracking device is shipped to the Participating Entity's location with the standard, reusable, adjustable strap already connected and is immediately ready for easy installation without the use of any tools.

SHADOWATCH (OPTIONAL)

The installation process for the ShadoWatch is quite simple and takes only minutes to install. The device should be assigned to the participant in the monitoring database and the battery should be fully charged prior to installation. To begin the installation process, one side of the strap is locked onto the device housing by attaching it with two (2) screws. The strap is then sized by placing the ShadoWatch and strap around the participant's wrist. One finger width should be between the strap and the participant's skin. Once the proper size is determined, the excess strap is removed and the device is installed by inserting the two (2) remaining screws into the open end of the strap and the device housing. Once the device is locked in place on the participant's wrist, security covers are then snapped in place to cover the screws on each side of the device housing.

- Tracking device must offer at least two (2) types of tamper notification.

SENTINEL RESPONSE

OM500

The OM500 GPS tracking device detects **three (3) tamper types including 1) fiber-optic strap design strap tamper, 2) device tamper and 3) backplate tamper**. Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and dual pressure sensors within the device, **the OM500 device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tamper with the strap**. The monitoring system then immediately sends the alert to the appropriate agency-defined personnel. The OM500 device sends a tamper alert if the participant severs the strap or if the unit loses contact with the backplate, indicative that the device has been uninstalled/disassembled. Additionally, the unit will send a tamper alert if the

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



unit is broken/cracked or if the unit's backplate is separated from the rest of the device.

Once installed, attempts to defeat, remove, or tamper with the OM500 GPS tracking device will also be visually obvious to trained personnel. The rugged, re-useable 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 and the securing pins are both tamper evident.

The OM500 devices offer the most advanced tamper detection and reset methodology. If the agency officer is not near a computer, he or she may call the Sentinel National Monitoring Center to investigate or clear any tamper event. The smartphone-based DNA Mobile App is also available to allow Agency officers to clear alerts and access participant activity while away from the office.

—IMPORTANT SENTINEL ADVANTAGE—

Feature Advancements for OM500 GPS:

- + **Enhanced detection and reporting of device Potential Shielding:** The potential shielding of the OM500 is detected based on various parameters/characteristics of GPS, Cellular and Wi-Fi signals. The system analyzes the RF noise characteristics and levels along with knowledge of signals that are not present to identify if the lack of signal is due to the environment or due to shielding of the unit.
- + **Enhanced detection and reporting of device Potential Slippage:** In addition to the OM500's three (3) tamper types already developed and implemented, Sentinel has developed an even more robust approach to detect and report possible unidentified removal via the Potential Slippage alert. Within our internal firmware, Sentinel is maximizing the benefits of the OM500 internal components. By utilizing the accelerometer in combination with cellular signal measurement, "Tilt" measurements, Wi-Fi changes and GPS signal strength, we have developed an even more advanced tamper/removal detection solution to accompany our original leading edge tamper technology.

SHADOWWATCH (OPTIONAL)

The ShadoWatch is equipped with triple tamper detection including 1) fiber-optic strap design tamper, 2) device case tamper, and 3) proximity tamper. Within seconds the ShadoWatch generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and proximity sensors, the ShadoWatch device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tampers with the strap. The ShadoWatch device will send a tamper alert if the participant severs the strap or if they attempt to slip the device off their wrist by generating a Proximity Tamper. Once installed, if the participant tries to attempt to remove the ShadoWatch device by cutting it off, a Band Tamper Alarm will generate. Additionally, if they attempt to remove the device by trying to slip it off their wrist, a Proximity Tamper will alert to the unauthorized removal and supervising personnel will be immediately notified.

- On a full charge, the battery must, at a minimum, last 40+ hours. The device must charge to a minimum of 24 hours of battery life within one (1) hour and be fully charged in about three (3) hours.

SENTINEL RESPONSE

OM500

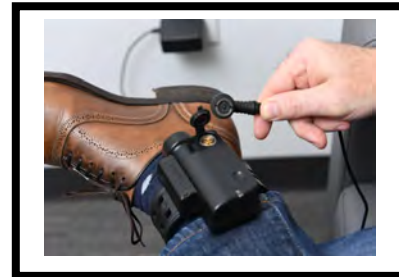
The **OM500 battery will last approximately 120+ hours (5+ days)** on a full charge on a standard rate plan. The OM500 requires **only 30 minutes of charging per day** to maintain battery life that exceeds five (5) days utilizing a charger that is plugged into a standard AC electrical outlet via power cord certified to UL standards and of extended length (approximately 10 feet long) to adequately connect to the household AC power. The OM500 can



be recharged from a depleted battery to 100% charge in one hour to one hour and ten minutes.

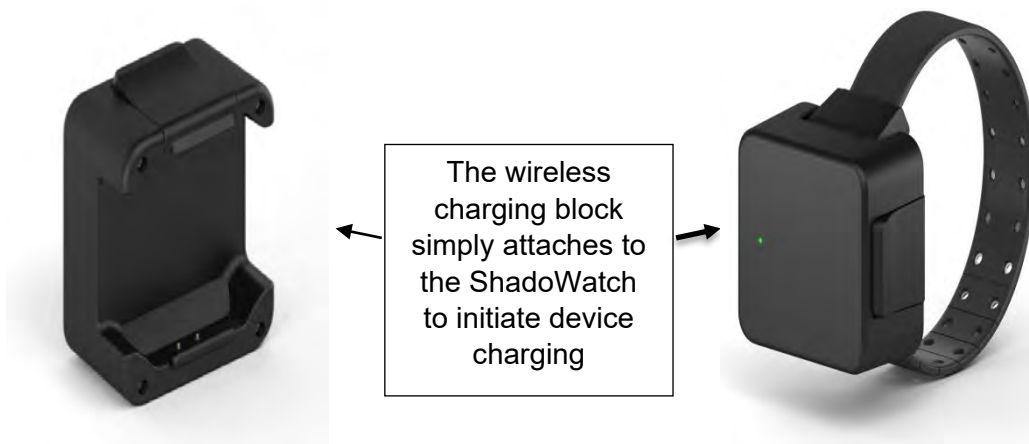
—IMPORTANT SENTINEL ADVANTAGE—

The OM500 features a magnetic charging connector that attaches and swivels 360 degrees to provide optimum connectivity and mobility for the participant and to avoid charger damage during charging sessions. **Unlike other device charging cords that lock into the charging port of the device, our design allows for it to disconnect if it is pulled on, so that damage to the device and charger is avoided.** The unit is equipped with an LED light that can be configured to flash **RED** when placed on the charger and turn off the LED light when removed from the charger. Additionally, audio commands announce charging starts and stops.



SHADOWATCH (OPTIONAL)

The ShadoWatch provides ample battery power and staff can be alerted if there are any Low Battery conditions that occur. The unit offers 24+ hours of battery life while providing 1-minute location intervals and 70+ hours of battery life while providing 5-minute location intervals. However, when using the remote charger (see below image) the ShadoWatch will continue to function as designed and provide more than 70 hours of optional battery life. The remote charger provides several days of charge capability and only requires a charging period of 90 – 120 minutes to be fully charged. The ShadoWatch is equipped with a wireless charger that simply snaps onto the watch allowing the participant to freely move around while charging. The wireless charging block simply attaches to the ShadoWatch to initiate device charging, as shown below.



- The beacon must ~~have at least three (3) range settings~~ be able to accommodate various sizes of residences. **[Edited per Amendment # 3, Scope of Work_ Revised 2.6.26~2]**

SENTINEL RESPONSE

OM500

The default range setting for the OM500 Beacon is approximately 75 feet, and the SentinelDNA monitoring platform enables a user-configurable, variable-range, Beacon Home Zone that is used in conjunction with the OM500 Beacon. This configurable Beacon Home Zone can be set to any radius to ensure curfew compliance. The use of Beacons with the OM500 is very uncommon as the OM500 GPS acquisition and triple location technology reduces GPS drift and provides accurate location information even in impaired locations. Officers are



also able to pair multiple Beacons to the same OM500, thereby increasing the range to accommodate various sizes of residences.

SHADOWWATCH (OPTIONAL)

The optional ShadowBeacon is designed for indoor tracking and acts like a traditional Radio Frequency (RF) device to always provide continuous monitoring. Often used in areas of impaired GPS signals such as inside large warehouse facilities or used to more tightly define/restrict a program participant's movement in smaller areas such as high-rise apartment buildings. The ShadowBeacon has three (3) programmable range settings to adjust to specific areas and can be paired with ShadoWatch. Features of the ShadowBeacon include:



- + Small design
- + Tamper-proof – detects if ShadowBeacon is moved
- + Mounts with adhesive strips to walls/ceilings
- + Completely self-contained – requires no AC power or telephone connectivity
- + Adjustable range settings

- ~~In addition to s~~ Standard AC charging ~~is required. Additional methods;~~ tracking device must have ~~additional ways of charging~~ such as an on-body charger (OBC) and/or USB port are acceptable.
[Edited per Amendment # 3, Scope of Work_ Revised 2.6.26~2]

SENTINEL RESPONSE

OM500

The OM500 features a magnetic charging connector that attaches and swivels 360 degrees to provide optimum connectivity and mobility for the participant and to avoid charger damage during charging sessions. Unlike other device charging cords that lock into the charging port of the device, **our design allows for it to disconnect if it is pulled on, so that damage to the device and charger is avoided.** The OM500 utilizes a charger that is plugged into a standard AC electrical outlet via power cord certified to UL standards and of extended length (approximately 10 feet long) to adequately connect to the household AC power.

In addition to standard AC charging, the OM500 ankle-worn GPS device can also be charged using an on-body charger (OBC). Sentinel's OBC is not required and used very infrequently due to the OM500's 5+ day battery life and quick charge capabilities. The OBC is a small, lightweight device easily attached to the OM500 unit worn by the participant to allow them to charge the device "on the go" without being tethered to a wall outlet affording the participant more freedom of movement.



OM500 GPS DEVICE SHOWN WITH THE ON-BODY CHARGER (OBC)

SHADOWATCH (OPTIONAL)

The ShadoWatch is equipped with a wireless charger that simply snaps onto the watch allowing the participant to freely move around while charging. The wireless charging block simply attaches to the ShadoWatch to initiate device charging. Also, available is a USB cable to charge the device via AC power.

Wired Charging: Direct Magnetic Connection



Mobile Charger: Direct Magnetic Connection



- The transmitter must be easily installed on the Client with minimal training and experience. Contractor must specify the tools required and procedures to install the transmitter. The Contractor must supply the tools and equipment necessary to install the transmitters and replace the transmitter straps, at no additional cost.

SENTINEL RESPONSE

OM500

The OM500 tracking device is easily installed by the trained Participating Entity officer in under five (5) minutes without cutting or specially designed tools. The OM500 GPS tracking device is shipped to the Participating Entity's location with the standard, reusable, adjustable strap already connected and is **immediately ready for**

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



easy installation without the use of any tools. The OM500 is extremely easy to attach to the participant's ankle with a heavy-duty reusable, adjustable and replaceable strap. The strap is designed and has been in use for over 10 years to provide a comfortable and secure fit with multiple sizing options to ensure the proper fit on each person. Two (2) locking pins connect the unit to the back plate. Once properly attached to the ankle, the device will immediately detect and report a tamper message if it is removed. The OM500 GPS tracking device strap is easily sanitized and reusable on multiple participants without the need for replacement. The standard sized strap fits 99% of the population and an extended length strap is available to accommodate the largest ankles. An optional cut-resistant strap is also available as an alternative to the OM500 standard strap. Sentinel will provide all tools and equipment necessary to install the OM500 transmitter and replace the transmitter straps at no additional cost.



SHADOWATCH (OPTIONAL)

The installation process for the ShadoWatch is quite simple and takes only minutes to install. The device should be assigned to the participant in the monitoring database and the battery should be fully charged prior to installation. To begin the installation process, one side of the strap is locked onto the device housing by attaching it with two (2) screws. The strap is then sized by placing the ShadoWatch and strap around the participant's wrist. One finger width should be between the strap and the participant's skin. Once the proper size is determined, the excess strap is removed and the device is installed by inserting the two (2) remaining screws into the open end of the strap and the device housing. Once the device is locked in place on the participant's wrist, security covers are then snapped in place to cover the screws on each side of the device housing. Sentinel will provide the screwdriver and scissors for device installation at no additional cost.



B. GPS Software

B. Software Requirements.

- GPS services must include a monitoring system that is capable of being accessed through a secure (password protected) internet connection and fully supported by a secure database for transactional records. GPS receiver must be capable of communicating with the U.S. Government Global Positioning System. The service must be inclusive of all technology, equipment, systems, and related support services, and must be fully supported by twenty-four (24) hour monitoring services and staff.

SENTINEL RESPONSE

OM500

Sentinel's proposed GPS services include our proprietary DNA monitoring system that is accessed through a secure internet connection (multi-factor authentication through a Two-Factor Authentication (2FA) that requires two distinct factors to verify a user's identity, such as a password and a one-time code) and fully supported by a secure database for transactional records. The Sentinel proposed monitoring applications operate in a secure, highly reliable, redundant, and scalable infrastructure. The data center environment was designed with security, redundancy and continuous operations in mind at every layer. In addition to steps taken to detect and prevent misuse or tampering of Sentinel's products and services, the platform is deployed at multiple data centers to provide geographical redundancy. Data is continuously replicated from the Primary to the Secondary data center providing failover redundancy whenever needed. The infrastructure is designed with a high-availability storage area network (SAN) containing redundant and automatic iSCSI pathing across multiple network interfaces, multiple network switches, and all flash SAN storage managed by redundant SAN controllers. The datacenter operations are monitored and supported by Sentinel employed hardware and software engineers 24/7/365 to ensure continuous operation and maximum uptime.

The OM500 GPS tracking device communicates with the 32 U.S. Government global positioning system satellites, including the GPS, Galileo, GLONASS, and BeiDou satellite constellations. The unit is equipped with multiple channels in order to rapidly scan the horizon to determine its location from the visible satellites in orbit. Sentinel's central host system securely communicates data and receives data from the proposed GPS devices via cellular communications. Each of the OM500 GPS units are available in either Verizon or AT&T LTE cellular data carriers to securely communicate data and receive data from Sentinel's DNA, our proprietary monitoring application. Communication between the OM500 GPS device and the cellular carrier transmits through a secure, encrypted tunnel. This communication then posts over an HTTPS connection to Sentinel's monitoring system. Once posted to the system, the data is then viewable to authorized users through the DNA monitoring application.

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year with bilingual staff available at all times.

SHADOWWATCH (OPTIONAL)

As an option to those Participating Entities that desire a wrist worn GPS device for client populations that may not be able to wear an ankle device, Sentinel is offering the ShadoWatch for these occasions.

ShadowtrackONE offers multiple security and/or permission levels. The system can enable two-factor authentication for user sign on and offer various permission levels that include the following: Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all pertinent participant information), UserReadOnly (can access the database but has no control to make any changes).



The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the agency's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

The ShadoWatch wrist worn GPS device is a continuous Global Positioning System (GPS) electronic monitoring solution that provides near-real-time reporting of individual locations within a range of plus or minus 10 meters outdoors and plus or minus 30 meters indoors. The ShadoWatch collects GPS location data once per minute and leverages GPS, Cellular, and Wi-Fi technologies to track program participants' locations for always-on, high-precision tracking. The ShadoWatch is designed to search for and utilize satellites from various global positioning systems, including GPS, BDS, GLONASS, and others. It automatically selects satellites with the strongest signals to ensure optimal performance. This advanced technology allows the watch to use more than three satellites simultaneously for accurate and reliable tracking. Sentinel's ShadoWatch incorporates multiple advanced technologies specifically designed to deliver a high degree of accuracy that automatically measures, calculates, and reflects any accuracy deviation in several feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby increasing officer confidence. ShadoWatch devices communicate using multiple cellular network providers and automatically switch between providers and their respective roaming partners' cellular networks based on service availability. This approach ensures that if one network was to fail, be unavailable or degrade; our electronic monitoring devices would automatically fail over to other operating networks.

- Web-based platform accessible via desktop, tablet, and mobile devices.

SENTINEL RESPONSE

OM500

DNA is a secure web-based application that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year via commonly used web browsers (e.g., Google Chrome, Microsoft Edge, etc.) over a high-speed internet connection. The SentinelDNA Monitoring System is designed to simplify access and usage across modern browsers on workstation computers and laptops (Windows, Mac OS X, Linux) and any mobile device (iOS, Android). The DNA monitoring application is 100% Internet-based and agencies do not need to purchase, install, or download any custom hardware or software components, applications, or client requirements. This advanced application improves the overall management of program information providing direct access to monitoring data for all Sentinel staff as well as authorized Participating Entity personnel.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application is a secure web-based monitoring software platform that is robust and user-friendly, allowing access over a wireless network 24 hours per day, 365 days per year without interruption. Whether the participant is installed on GPS Tracking Devices, Remote Alcohol Monitoring Devices, or App Related Services, the basic functionality of the system remains the same and everything is easily accessible in one complete software application via commonly used web browsers like Google Chrome or Microsoft Edge and is viewable via a desktop computer, tablet, or mobile device.



- Secure login with multi-factor authentication.

SENTINEL RESPONSE

OM500

Sentinel's proposed monitoring solution provides secure login with multi-factor authentication through a Two-Factor Authentication (2FA) that requires two distinct factors to verify a user's identity, such as a password and a one-time code. By enabling at least one of the methods below, the user's account will require 2FA to log in, and the user must authenticate when accessing the web application and mobile app via single sign-on (SSO). The monitoring solution supports two types of Authentication methods (1) Authenticator App and (2) Email.

- + **Authenticator App:** Authenticator Apps provide a Time-Based One-Time Password (TOTP), which is considered one of the more secure options compared to other two-factor authentication methods available. Many authenticator apps, such as Google Authenticator, Microsoft Authenticator, and FreeOPT, are available in the app stores for Android and iOS. Users must follow the Authenticator App's guidelines for installation and adding new accounts.
- + **Email OTP:** Another option available to users is to receive a one-time password (OTP) code in their email. Upon enabling this option, the system will send a code to the email address used to log in to the monitoring system account with their user ID.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring applications offers multiple security and/or permission levels. The system can enable two-factor authentication for user sign on and offer various permission levels that include the following: Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all pertinent participant information), UserReadOnly (can access the database but has no control to make any changes).

- Real-time data collection and display for all device types.

SENTINEL RESPONSE

OM500

DNA makes it easy for officers to access real time data collection and display for individual participants or their whole caseload from a secure environment. Designed with the needs of end-users in mind, DNA uses a straightforward, intuitive user interface that allows users to efficiently complete all monitoring tasks in real-time including:

- + Enroll a participant
- + Create/edit schedules
- + View, create notes
- + Clear events and alerts
- + Locate participants
- + Send custom messages to participant(s)
- + Store and view demographic information
- + Alert processing and advanced triage notification
- + Perform Analytics including Point Pattern Analysis
- + Verify and document every contact with participants while in the field
- + Inventory Management including Equipment Recovery Dashboard
- + Perform data management administration
- + Create and edit zones (inclusion and exclusion)
- + Adjust tracking rate plans
- + Review device battery status and charging events
- + Create and print reports
- + Store and view photos and documents
- + Victim assignment and notification
- + Perform audits
- + Perform Event Detection

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Sentinel's monitoring system records all data with a historical transaction record and is stored/archived for retrieval/backup in a database when requested by agency personnel. SentinelDNA Monitoring Application maintains a permanent searchable and reportable record in the form of a: 1) Client Audit Report; and 2) User Audit Report. In addition, all monitoring events and notifications are logged with date and time stamp and are also available for auditable review.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application offers real time active GPS data collection and display for all device types. Authorized staff will be able to efficiently access, review, and complete all monitoring tasks in real-time including:

- + Single point of data entry
- + Dashboard View
- + Enroll a participant
- + Create/edit schedules
- + View, create notes
- + Locate participants
- + Scheduling of events
- + Review alerts
- + Access Knowledge Base that allows users to easily pull up help topics related to defined training tips
- + Access supervisory tool for entries and edits
- + Store and view photos and documents
- + View GPS Mapping
- + Inventory control
- + Access & Review Automated and Ad Hoc Reports
- + Review Event History
- + Client deactivation
- + Create & Review Analytics

- Customizable dashboards with mapping tools and client history.

SENTINEL RESPONSE

OM500

Customizable Dashboard

DNA provides customizable dashboards with mapping tools and client history. 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 each participant. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, location information (via mapping), equipment status, current battery status, as well as zones and daily curfew schedules.

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT DASHBOARD SCREEN

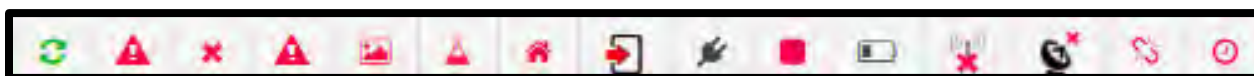
Dashboard

Home - System Overview

Name	ID	Type	Deployment	Compliance	Battery	Profile	Officer
Anderson, Chad Verizon Test	Q1800044	CM				Web Only	Owen County
BART, Amy	Q1800055	CM				web Only	Amy Richards
BART, DJ	Q1800093	BART				Voice County	DJ Sales/Demo
BEACON, BJ	Q1800057	(GPS)/BEACON				Web Only	Mark Contestable
Brown, Steven Sprint Test	Q1800046	CM				Web Only	Owen County
Contestable, Mark A	Q1800050	CM				web Only	MARK CONTESTABLE
Dean, Mike DCPSA	Q1800080	GPS				DC TEST	Mike Dean
Hodges, Tia Sprint Test	Q1800043	CM				Web Only	Owen County
HomeNet, Jeremy	Q1800054	RF				SALES - Bringham County Sheriff's Office - DO	Jeremy Kenedel
RF Patrol, DJ	Q1800047	RF				Voice County	DJ Williamson
Shuts, Patrick verizon test	Q1800045	CM				Web Only	Owen County
Test, DCPSA	Q1800041	GPS				Web Only	Mike Dean
Test, DCPSA	Q1800042	GPS				Web Only	Mike Dean
Tracker, John	Q1800056	GPS				SALES - Bringham County Sheriff's Office - DO	Amy Richards
WILLIAMSON, D J	Q1800092						DJ Williamson

Showing 7 of 15 of 15 entries

Authorized users can refine the information displayed by clicking any of the dashboard headings (Name, OID, Type, Equipment, etc.) in order to re-sort the information based on that parameter. This allows agency staff to quickly view participants by type of monitoring, by alert, or even by battery percentage. In addition to sorting the information by column, icon buttons (shown below) displayed at the top right of the Dashboard allow the user to filter participants based upon the selected criteria such as displaying all participants who have a Tamper alert by selecting the Tamper icon.



Below the sort icons, DNA has a local search option (shown below) to make it easy to refine the dashboard display to specific participants using a first or last name. This allows the user to quickly locate a participant without scrolling through the full caseload list.

Search Clients

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

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT ACTIVITY SCREEN

Client Personal Info		Client Equipment Info		Agency	
OID	ID6719830	Type	GPS	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT000000	Officer	Training Department
Name	HELM Tester, AT&T OM500	IMEI	10000809	Cell Phone	714-726-1114
Home Ph	(800) 589-6003	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csuazo@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Simon Ct, Anaheim, CA 92805			Support Staff	None
Timezone	PST			Timezone	PST

Event	Event Time	Received Time
Work Failed To Enter Inclusion Zone	10/21/2025 8:30:10 AM	10/21/2025 8:30:09 AM
Work Late To Enter Inclusion Zone	10/21/2025 8:20:24 AM	10/21/2025 8:20:23 AM
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
KMTR Tamper - GPS	10/21/2025 8:02:20 AM	10/21/2025 8:02:47 AM
Backplate Tamper	10/21/2025 8:02:20 AM	10/21/2025 8:02:46 AM

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. **This provides all the important participant information on one screen.**

DNA CLIENT EQUIPMENT STATUS SCREEN

Client Personal Info		Client Equipment Info		Agency	
OID	ID6719830	Type	GPS	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT000000	Officer	Training Department
Name	HELM Tester, AT&T OM500	IMEI	10000809	Cell Phone	714-726-1114
Home Ph	(800) 589-6003	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csuazo@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Simon Ct, Anaheim, CA 92805			Support Staff	None
Timezone	PST			Timezone	PST

Status	Event Time
HOME	Since 3/14/2025 8:03:46 AM
GPS(Strap) Tamper	10/20/2025 6:05:29 PM Clear
BackPlate Tamper	10/20/2025 6:05:29 PM Clear
Potential Shielding	
Potential Sippage	
MEZ Enter	

As illustrated in the Equipment Status screen image above, the client's current location is shown on the map to the lower left along with the current status of the device including any tampers along with the date and time of occurrence. Officers can quickly view if there is a device issue without wasting time.

Mapping Tools

Sentinel's DNA utilizes Google Maps® which provides automatic updates to the system always delivering the latest maps and upgrades. DNA tracks its own points and overlays the points on the most recent Google Maps®

Request for Proposals for
ELECTRONIC MONITORING

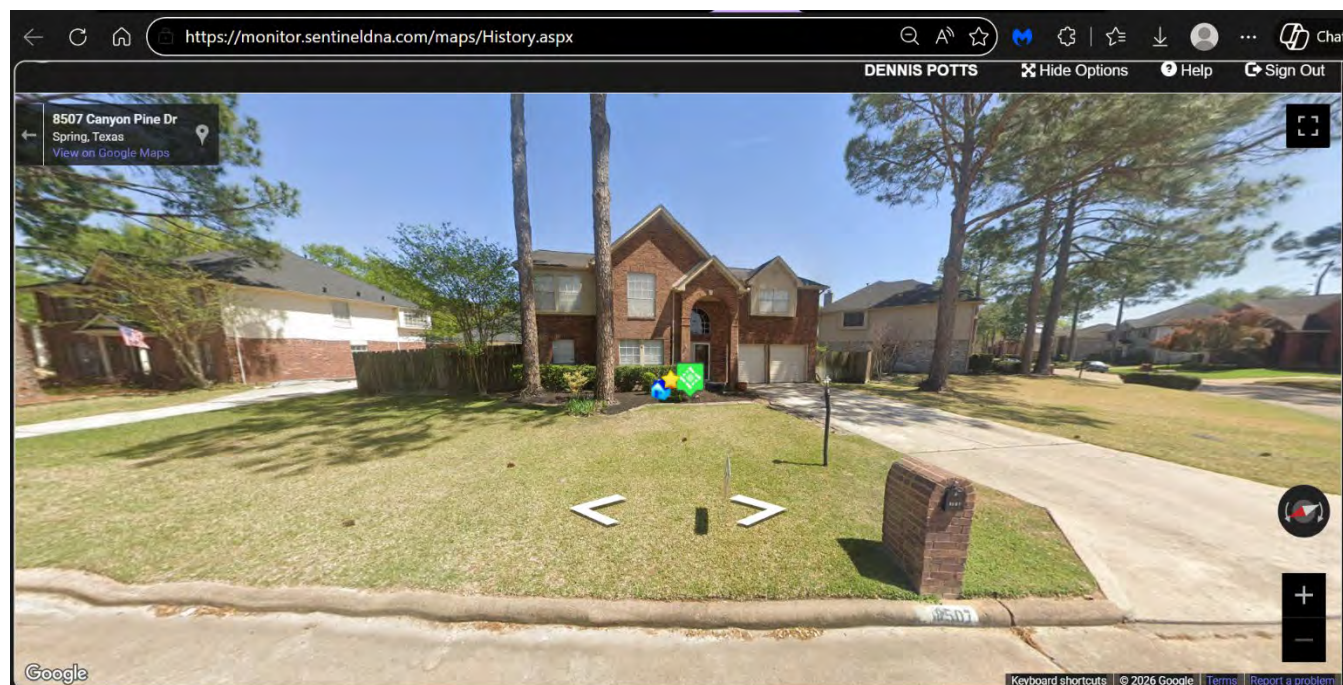
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



available at the time of 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). There are also multiple distinct views including traditional, bird's eye, and street view. These interactive maps contain easily recognizable images at the global level as well as down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking data on the map. With the click of the mouse button, DNA allows authorized users to "drill down" from a high-level view of a participant's overall tracking down to his/her tracking movements at a specific location.

DNA STREET VIEW USING GOOGLE® MAPS



Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA offers several mapping utilities that allow authorized users to customize the mapping tools to better suit their needs. **Map Utilities** allow users to center the map around a specific address while **Map Settings** allows the user to enable or disable a variety of map features.

- + **Show client track:** Connects points during playback to illustrate the order.
- + **Show track direction:** Adds arrows to the client track to indicate participant direction.
- + **Center map while animating track:** Centers the map on each point during playback.
- + **Filter points while the client is HOME:** Hides points collected while the participant was within the HOME inclusion zone.
- + **Show Template Zones:** Place an icon on the map for each template zone assigned to the participant.
- + **Show Individual Zones:** View or hide individual zones on the map when viewing the participant's location.
- + **Stack Points:** Groups consecutive points located in the same geographical area.
- + **Show Numbered Labels:** Enables the chronologically numbered labels on the points
- + **Show GPS Accuracy:** Enables the GPS Point Accuracy Filter
- + **Show Locations Labels:** Allows to hide locations pin on the zone map view.
- + **Grid Size:** Adjust the size of the area in which the points should be grouped as one stack.
- + **Stack Min Duration:** Filters out locations where the participant was present for less than a specific time duration.

A screenshot of the "Map Settings" dialog box. It contains a list of settings with checkboxes. The settings are: "Show client track" (checked), "Show track direction" (checked), "Center map while animating track" (checked), "Filter points while client is HOME" (unchecked), "Show Template Zones" (unchecked), "Show Individual Zones" (checked), "Stack Points" (unchecked), "Show Numbered Labels" (checked), "Show GPS Point Accuracy" (checked), and "Show Location Labels" (checked). At the bottom, there are two input fields: "Grid Size" with the value "100" and "Stack Min Duration" with the value "0".

Client History

—IMPORTANT SENTINEL ADVANTAGE—

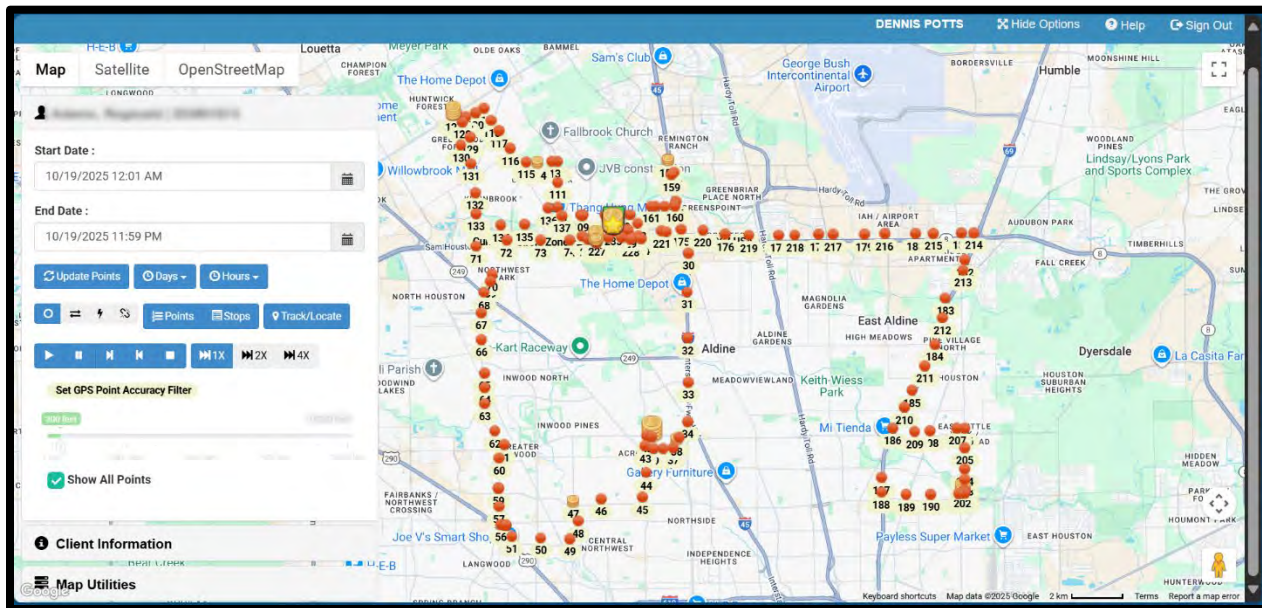
As an added service feature, DNA allows authorized users to view the actual movements of the program participant, including the time of those movements, in a visual map and in report format. By clicking *Update Points* after selecting a date and time range, **the user can view a point animation / DVD-style playback with fast-forward and rewind buttons**. Tracking data is plotted on the map in numerical order of occurrence allowing for ease of viewing and during playback, the address, time of the location point, latitude and longitude of the location, and the speed at which the participant was traveling are all displayed beneath the playback controls. The screen below displays a participant's location history.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA VIEW CLIENT LOCATION HISTORY SCREEN



SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application includes an existing dashboard that can be further customized to meet the specific needs of the Participating Entity. The systems include mapping function that allows an authorized officer to filter tracking data by specific date and time periods and offers an automatic playback feature when reviewing participant tracking history.

Upon logging into the system, authorized users are immediately taken to the dashboard screen which displays all program participants, as well as alarm details, last known tracking points, device type, etc. This data can be filtered by All Active Participants and/or only by those assigned to the officer's caseload. A map can be displayed showing all active program participants' locations on a single map allowing supervising personnel to quickly ascertain if any participants are in or out of program compliance. The Dashboard also contains an Officer's Portal in which App Related Functions can be performed. Whether agency personnel want to place a video call with a participant, perform an On-Demand Location Check, perform a Secured Chat Session with a participant, send a Mass Notification message to all program participants, etc. – **all functions and features are right at the user's fingertips in one easy to use software platform.**

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SAMPLE DASHBOARD SHOWING FEATURES AND FUNCTIONS

The screenshot displays the Shadowtrack dashboard interface. At the top, the user is logged in as 'Shadowtrack | McAndrew, Tom (Shadowtrack)'. The dashboard shows a 'Sales Demo' section with a search bar and a 'Parent: Shadowtrack' label. Below this, there are tabs for 'Enrollees', 'Users', 'Contacts', 'Offenses', 'Protocol Groups', 'Billing', 'Settings', 'Zones', 'Sub-Entities', 'Schedule Templates', 'Interview Protocols', 'Check-Ins', and 'Resources'. The 'Enrollees' tab is active, showing a list of three enrollees:

Enrollee	Enrollee ID	Assigned Officer	Alarms	Info
Demo (Ankle), McAndrew	521534460	McAndrew, Tom (Shadowtrack)	2 Alarm(s) Protocol: McAndrew Agency Unwire Protocol	ShadowDevice Battery: 94% Last Comm: 8/19/2024, 1:02 PM
Demo (ShadowPhone/Tether), McAndrew	521546726	McAndrew, Tom (Shadowtrack)	1 Alarm(s) Protocol: McAndrew Device (ShadowPhone)	ShadowPhone Battery: 75% Last Comm: 8/19/2024, 1:00 PM
Demo (Watch), McAndrew	521535226	McAndrew, Tom (Shadowtrack)	2 Alarm(s) Protocol: McAndrew Agency Watch Protocol	Mobile Without App ShadowWatch Battery: 87% Last Comm: 8/19/2024, 1:02 PM

Participant Profiles (Accessing and Adding Profiles)

It is extremely easy to access or add participant profiles in the monitoring database. To access an existing participant profile, simply click on the individual's name on the Dashboard or an officer can access this information by clicking on the Participant icon in the left portion of the screen which displays various menu items. Once selected, the officer will see all the pertinent information as it pertains to the individual participant. **Whether setting up a participant on GPS monitoring or App Related Services, the process remains the same.**

The screenshot displays the Shadowtrack participant profile page for 'McAndrew, Tom (Shadowtrack)'. The page is divided into two main sections: 'Basic Information' and 'Enrollment'. The 'Basic Information' section includes fields for First Name, Middle Name, Last Name, Suffix, Email Address, Date of Birth, Language, Time Zone, Internal ID, Primary ID, and a photo. The 'Enrollment' section includes fields for Active status, Active Start Date, Active End Date, Enrollment Password, Date of Voice Enrollment, Date of Facial Enrollment, and TFN Opt Out Date. There are buttons for 'Edit', 'Show History', 'Update Active Dates', 'Reset Enrollment', and 'Enrollment Form'.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



To add a new participant into the database, click on the +Participant tab and follow the quick and easy five (5) step process: Step (1) – Participant Info, Step (2) – Case Info, Step (3) – Add Services, Step (4) – Add Zone, Step (5) – Add Schedules.

Tracking Details with Google Maps

Tracking data is achieved through the ShadoWatch devices' ability to obtain location through GPS Satellite data and Wi-Fi data, as well as Location Base Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the devices are in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS nor Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located. Additional details such as battery percentage, speed of travel and direction of travel are also displayed. The mapping function allows the officer to filter tracking data by specific date and time periods and offers an automatic playback feature when reviewing tracking data. **Once again, reviewing tracking details on participants whether they are on GPS Tracking or App Related Services remains the same - thus making reviewing participant location data very simple.** Indicated on the next page are examples of the level of tracking detail obtained:

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Date Range
Custom

Filter Start (User Time)
12/10/2023 2:00 PM

Filter Start (Enrollee Time)
12/10/2023, 2:00 PM

Export

Filter End (User Time)
12/10/2023 5:00 PM

Filter End (Enrollee Time)
12/10/2023, 5:00 PM

Maximum 250 locations displayed

1 to 5 of 173

1	12/10/2023 04:59 PM EST	Address	GPS Speed: 38.66	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
2	12/10/2023 04:57 PM EST	Address	GPS Speed: 37.48	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
3	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
4	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
5	12/10/2023 04:55 PM EST	Address	GPS Speed: 33.37	Battery: 81 Charging: No Signal Strength: 66 Zone Status:

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- Automated notifications and alerts (via SMS, email, or in-platform) for violations such as curfew breaches, tampering, or low battery, and any other alerts as defined by the Participating Entity.

SENTINEL RESPONSE

OM500

Sentinel's DNA web-based information system is also equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts / notifications and violations such as zone breaches, curfew breaches, tampering, or low battery, or any other alerts as defined by the Participating Entity. Violations can be prioritized to alert immediately or hold for a grace period. The DNA Profile Manager allows for automated (text/email/in-platform) notification of alerts as well as optional manual operator escalation/closed loop communication and sequencing. The Profile Manager also differentiates protocol changes within a single alert by time and day of the week. Please refer to the image below for Sentinel's **Notification Procedure** screen within DNA. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

The screenshot shows the 'Profile Viewer' interface for a profile named 'Do Not Pass Go Bonding (Version: 1)'. It displays a sequence of steps for two days: Sunday and Monday. Each day has a table with columns for 'State', 'Action', 'State Time', and 'Next State'. The steps include 'Auto Email and McApp', 'Delay', and 'McApp'. Instructions for each day are provided below the tables. A 'Back to Profile Manager' button is visible in the top right corner.

Click here to go back to Synergy

Sign Out

Profile Viewer

Home Profile Viewer

Do Not Pass Go Bonding (Version: 1)

Created on 3/21/2024 8:15:26 PM

Back to Profile Manager

Backplate Tamper - GPS11

Steps Clearing Alarms

Day: Sunday
Time: 00:00:00 - 23:59:59

State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Emails: abyss@sentrak.com			
Instruction: Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue.			
Step 2	Delay	10	Step 3
Step 3	McApp	0	
Emails: abyss@sentrak.com			
Instruction: If no tamper clear, contact officer on duty at the number provided. Close.			

Day: Monday
Time: 00:00:00 - 23:59:59

State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Emails: abyss@sentrak.com			
Instruction: Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue.			
Step 2	Delay	10	Step 3
Step 3	McApp	0	
Emails: abyss@sentrak.com			
Instruction: If no tamper clear, contact officer on duty at the number provided. Close.			

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application can be set up to handle Automated notifications and alerts (via SMS, email, or in-platform) for violations such as curfew breaches, tampering, or low battery, and any other alerts as defined by the Participating Entity. Each violation can be set up to have customizable Protocol Steps for each individual violation, as well as multiple manners in which notifications can be set up for the ShadowtrackONE monitoring application to automatically process according to the User Agency policies and procedures.

The below image details how to add a Protocol step and the image on the following page details how each protocol step can be fully customized.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Massachusetts Probation Service (MPS) Demo | Demo Officer, MPS

Alarm Type: Within Exclusion Zone | Grace Period (minutes): 0 | Active: ☒ | Auto-Resolve: ☐

Alarm Protocol Steps

+ Step

Protocol Action	Step Type	Recipient Type	Full Name	Message
Send SMS	Automated	Assigned User		Enrollee: __EnrolleeName__ Alarm Type: __AlarmType__ Alarm Triggered Date/Time: __DateTime__ Zone: __Zone__ Assigned User: __AssignedUser__
Send Message To Device	Automated			You have entered an unauthorized area. Leave the area immediately!
Place Call With Delivery Confirmation	Automated	Assigned User		This is the MPS Elmo Center calling in regards to program participant __EnrolleeName__ from __TenantName__ had a __AlarmType__ violation.

14 1 to 3 of 3

Clear Protocol Steps

+ Step

Protocol Action	Step Type	Recipient Type	Full Name	Message
Send SMS	Automated	Assigned User		Enrollee: __EnrolleeName__ Alarm Type: __AlarmType__ Cleared Date/Time: __DateTime__ Zone: __Zone__ Assigned User: __AssignedUser__

If automation is chosen in a Protocol Step (i.e. Place Call with Delivery Confirmation), the system can be set up to place a call in the following manner: to the Assigned User, to the Participant, to the Tenant Admin, to Other, and/or to a Contact.

Alarm: Within Exclusion Zone

Step Type: Alarm

Action: Place Call With Delivery Confirmation

Action Type: Automated

Recipient: ☒ Assigned User ☐ Enrollee ☐ Tenant Admins ☐ Other ☐ Contact

Available Mail Merge Fields:

- __AlarmType__
- __EnrolleeName__
- __TenantName__
- __ProtocolGroupName__
- __LastLocation__
- __Zone__

Note: The below text will be played after, "Hello. This is an automated notification" and before "Please acknowledge receipt of the message by saying 'Acknowledge' or by pressing any key."

Message: This is the MPS Elmo Center calling in regards to program participant __EnrolleeName__ from __TenantName__ had a __AlarmType__ violation.

Save Cancel

The ShadowtrackONE monitoring application incorporates optional advanced automated processes and voice options to be utilized to assist and aid in monitoring procedures. Alarm protocols can be customized based on the User Agencies desired alarm notification preferences ranging from email/text messages to automated voice notification options that allow delivery receipt confirmation.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Protocols are set up according to agency specifications which notify staff (as well as participants if so desired) of violations through designated notification methods.

Notification Options and Methods:

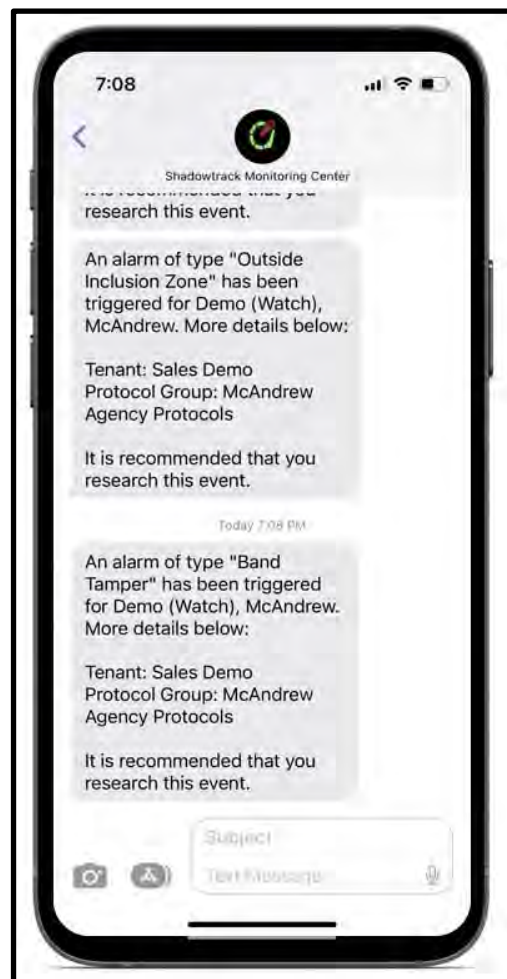
- + Send Text Message To Device
- + Send Email
- + Send SMS (Text Message)
- + Place Call
- + Place Call With Delivery Confirmation

Advanced Calling Automated Notification Options:

If "Place Call" is chosen, a phone call will be placed to any or all of the following:

- + Assigned User
- + Participant
- + Tenant Admin
- + Other (i.e. Victims)
- + Contact

The phone call will state *"Hello, this is an automated Shadowtrack notification. The program participant [John Doe] for [XYZ Agency] had an [Alarm Type] violation"*. Additionally, if "Place Call With Delivery Confirmation" is chosen, the message will go on to state *"Please acknowledge receipt of the message by saying Acknowledge or by pressing any key"*. If the violation is not acknowledged, a roll over person(s) can be contacted until acknowledgement is properly received.



- Reporting capabilities with customizable fields, exportable in PDF, Excel, and CSV formats.

SENTINEL RESPONSE

OM500

SentinelDNA is designed and maintained entirely by Sentinel's in-house IT Team, thus reports with customized fields are available upon customer request. SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

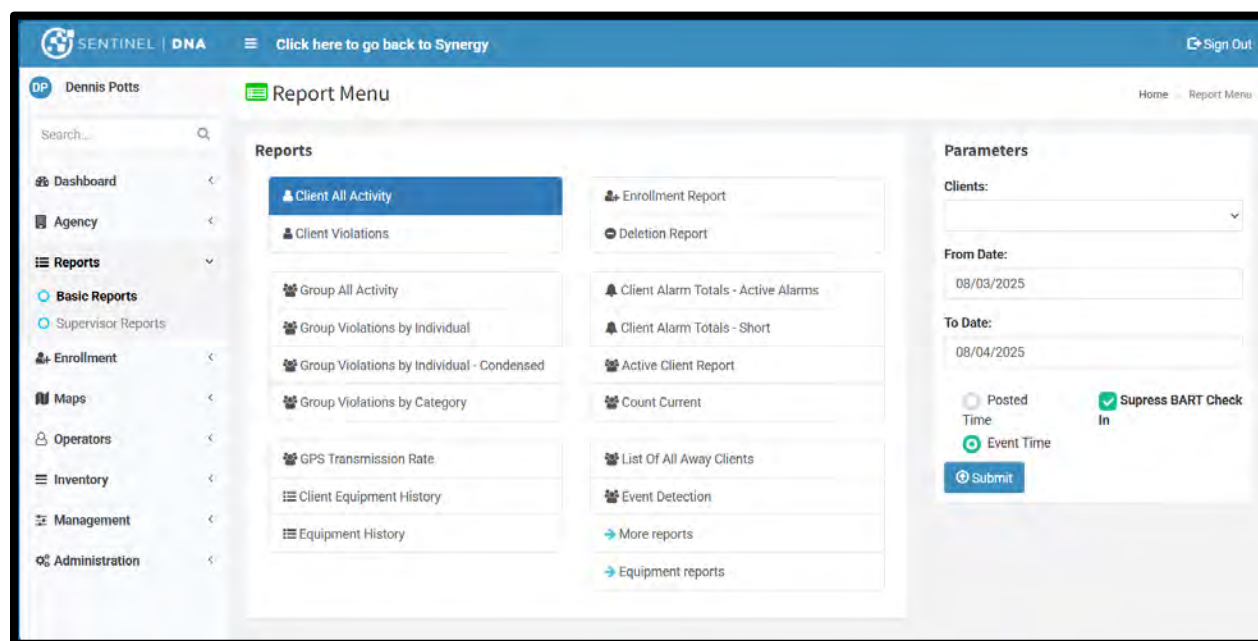


Separated Values (CSV) formats. Reports can be delivered as “Subscriptions” to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

DNA REPORT MENU SCREEN



If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

—IMPORTANT SENTINEL ADVANTAGE—

DNA provides additional reporting features for participants who are being tracked with GPS. From the Reports menu and the mapping screen, authorized users can run reports for a single participant or group of people:

- + Alerts showing which actions were taken and whether the notifications were successful
- + Reports showing all events, including alerts
- + Proximity, allowing users to see whether any or all participants were near a specific location at a specific time (Event Detection / Crime Scene Correlation)
- + Zone activity to show which participants entered and exited zones, such as AA, shopping malls, known drug areas, etc.
- + Stops Report that shows where and when participants stayed in one (1) location over a given time period
- + User Audit Report that shows which users are logging into the monitoring system and for how long



SHADOWATCH (OPTIONAL)

The ShadowtrackONE monitoring application has a wide array of report options ranging from violation reports to inventory control that can be downloaded, printed, and/or exported in various formats including exportable in PDF, Excel, and CSV formats. From within the monitoring platform, agency personnel can easily review/download/print/export the activity of a single participant or generate additional reports specific to the agency needs. Many of the reports already available were requested by current customers, including the following.

- + Alarms report
- + Charging History Report
- + Locations Report
- + Visit Points Report

Visit Points are generated in the system based on the following:

- + Minimum of 2 location points
- + Within a 3-minute period
- + Within a 50m radius

The Visit Points Report has been described by current agency users as being very helpful as it gives details including a specific location's arrival time, departure time, duration (in mins), the location address, and the latitude and longitude.

If the agency is in need of additional reports, our customer service and software development teams will work together to get anything else that may be needed or requested by the agency at no additional cost.

- Integration options with existing case management systems through APIs.

SENTINEL RESPONSE

OM500

Sentinel has developed and does support **Application Programming Interfaces (APIs)** to interface our SentinelDNA system with external systems. The Sentinel Software Development Team has extensive experience in developing and testing APIs, using best in class software development practices and tools such as Postman and REST Assured, and JMeter performance/load testing, to develop and test secure, robust and scalable API interfaces. Key technologies used include REST, JSON, JWT, and Webhooks.

Implementing an API would require an engagement between Sentinel and the contracting State's technical team(s) to understand the exact requirements, project scope, and infrastructure needs to implement the APIs and requested integration with a State's Offender Management System. Upon completion and agreement on the Project Scope Document, Sentinel would deliver the necessary API and/or integration for the contracting State and support our portion of this project to ensure system performance and uninterrupted data exchange.

SHADOWATCH (OPTIONAL)

The ShadowtrackONE monitoring application is capable of being integrated with existing case management systems through the use of an Application Programming Interface (API). Software integration typically refers to the process of combining separate software programs or elements into one system. The level of integration can



range from the combination of components that are relatively small to larger systems of significant size and complexity. Typical integrations allow two (2) databases to share information in order to maximize efficiency. Additionally, Shadowtrack's monitoring application would be able to export items such as Violations, Violation Notes, etc. without the need for agency personnel to enter this information into both databases.

- Audit trail and data retention in compliance with CJIS security requirements.

SENTINEL RESPONSE

OM500

Sentinel has designed the system, operations, and policies to align with CJIS requirements maintaining a complete audit trail for all device events, alerts, user actions, and monitoring results. Every action is time-stamped and retained according to strict data-integrity controls. The system's security and data-management framework are aligned with criminal-justice security expectations, providing full traceability for evidentiary purposes and long-term data retention requirements. All changes to participant or demographic information or monitoring data are saved within the system. Additionally, each employee has specific login credentials that permit Sentinel to perform detailed audits on user access to all participant records in the database to confirm that unauthorized changes have not been made. Additionally, our systems allow Participating Entities and their Supervisors to determine if an officer/user accessed any portion of our DNA system while monitoring the length of time the officer spent on the specific DNA module. This audit capability allows Supervisors to ensure officers are accurately reviewing tracking data and responding appropriately to program violations and participant activity.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with an agency's existing case management system. The ShadowtrackONE platform is accessible to authorized personnel needing participant access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity. The system includes the ability to provide and monitor audit trails throughout the application.

- Role-based access controls for administrators, supervisors, and officers. The system must provide security features, which must prevent unauthorized individuals from accessing any information held by the Contractor. Secure access to the system must be maintained at all times.

SENTINEL RESPONSE

OM500

The Company enforces role-based access control (RBAC) for access to systems and data through centralized identity and access management. Access is granted only to pre-defined roles aligned to job responsibilities and the principles of least privilege and need-to-know, with documented approval from designated system/data owners. Privileged and administrative access is tightly restricted (including the use of MFA for privileged and remote access), and role assignments are reviewed at least quarterly and upon personnel or job changes, with prompt removal upon termination. Access provisioning, changes, and administrative actions are logged and monitored to support auditability and align with NIST SP 800-53 Moderate access control objectives (e.g., AC-2, AC-3, AC-5, AC-6).



Sentinel's DNA Monitoring Application offers hierarchy user levels that will allow the system administrator the ability to limit the tasks available to a particular user and/or group of users through role-based access controls. DNA will enable the designated system administrator to set access levels for each authorized user. Additionally, the system administrator will have the ability to establish access levels to specific caseloads or groups in any combination for authorized users. The system administrator will have the ability to secure and restrict, or alternately enable, access to clients and their information.

Secure access to the monitoring application is maintained at all times. The system is completely secure and uses state-of-the-art security measures. Login authentication is based on NIST SP 800-63-3 Digital Identity Guidelines to ensure secure access to the Monitoring System. Sentinel has employed the use of Single Sign-On (SSO) and Multifactor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.

The DNA Monitoring Application and Case Management Software were designed and are managed based on following NIST SP 800-53 requirements. Sentinel's security staff members have worked within the NIST 800-53 related standards and frameworks since 2009 and have received accreditation for NIST 800-53 compliance for past contracts and products. Sentinel conducts yearly penetration tests and vulnerability assessments to prioritize needed security improvements and remediations. Sentinel uses NIST 800-53 as the basis for information system policies to ensure federal standards are being met or exceeded. Sentinel partners with a 3rd party Security Operations Center (SOC) provider to achieve 24x7 Managed Detection and Response security monitoring of endpoints and network traffic. Sentinel's staff and security partner monitor security bulletins for emerging threats, 0-day vulnerabilities, and new CVEs with immediate priority for any needed remediation on Sentinel's system. Our SOC partner also provides Managed Risk Continuous Vulnerability Scanning of internal and external surfaces, as well as Managed Security Awareness training and phishing simulation for all employees. Sentinel's staff monitors dark web malicious actor blogs, forums, and databases for information and credentials related to Sentinel's systems.

Sentinel maintains an aggressive posture of cybersecurity diligence with an ongoing focus on continuous improvement of security operations. Components of Sentinel's applications are hosted in the Oracle Government Cloud Infrastructure. The U.S. Department of Defense, intelligence community, and federal civilian agencies rely on Oracle Government Cloud. Oracle US government cloud infrastructure meets the standards DoD DISA IL 5, 4, 2, FedRAMP-High, FIPS 140-2 for cryptographic modules and is VPAT section 508 compliant. All externally facing HTTPS endpoints require TLS 1.2 or TLS 1.3 and are configured to prefer AEAD cipher suites (AES-GCM/ChaCha20-Poly1305). This ensures strong session confidentiality (including AES-256 where negotiated), integrity protection, and forward secrecy, aligned with widely accepted modern TLS hardening guidance.

Sentinel protects the perimeter of the data center and office networks with Fortinet FortiGate firewalls with Intrusion Detection and Intrusion Prevention features enabled and tracked. Security and Traffic activity is logged and ingested into the Arctic Wolf SIEM for combined Managed Detection and Response (MDR). Combined with the SentinelOne XDR Endpoint Protection Platform that runs on all Sentinel's servers and employee workstations and laptops, the Arctic Wolf 24x7 operated MDR service provides 24x7 rapid detection and reaction to intrusions.

Sentinel does not allow vendors or 3rd party access to participant data. Sentinel staff and end users (agency officers) access participant data using multi-layered login passwords. All activities conducted in DNA are recorded with date, time stamp, and user credentials to provide audit capability, replay of events, and access to historical accuracy.

SHADOWATCH (OPTIONAL)

The ShadowtrackONE monitoring applications offers multiple security and/or permission levels. The system can enable two-factor authentication for user sign on and offer various permission levels that include the following:



Installer (only has access to perform installation functions), TenantAdmin (has full administrative and set up access), User (officer level access to all pertinent participant information), UserReadOnly (can access the database but has no control to make any changes).

Network Security and Redundancy

The ShadowtrackONE monitoring platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the Participating Entity's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing access by computer and user/officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

AWS Hosting Services

The ShadowtrackONE monitoring platform is secure with Amazon Web Services (AWS), with servers located in different regions of the United States. Shadowtrack's activity is cloud-based, and access to the case management system or any of the raw data requires two-factor passcode identification and authorization along with other security measures. Operating with various locations worldwide, Shadowtrack accepts and follows each end-user's data and information record retention requirements.

Scalability and Reliable Access

Shadowtrack automatically adjusts to traffic changes to make sure the ShadowtrackONE platform is always up and running for the agency's needs. By spreading resources across multiple AWS zones, Shadowtrack's making sure that the system operates seamlessly and that it is always available – thus ensuring vital monitoring aspects always remain operational and continuous.

Cutting-Edge Data Management

Tracking location data for thousands of program participants is no easy task. With one GPS device set for one minute tracking – 1,440 location points daily or 525,600 location points annually are generated for just one program participant, resulting in an extensive amount of data to collect, process, and store. Behind the scenes, we're always refining how we store and manage this vast amount of data, so the agency gets the best experience. The ShadowtrackONE monitoring platform is supported by AWS and has the technology to ensure the agency gets the information it needs when needed.

SOC 2, Type 2 Compliance

Shadowtrack Technologies, Inc is certified by the American Institute of Certified Public Accountants (AICPA) to be Systems and Organizations Control (SOC) compliant. To that end, we meet or exceed **SOC 2, Type 2** compliance requirements.

- Tracking software must allow staff to enable GPS tracking in real-time and/or passive tracking.

SENTINEL RESPONSE

OM500

Via our secure, Internet-based SentinelDNA monitoring system, any authorized user can configure or change the data transmission rate plan (tracking and reporting intervals) from real-time and/or passive tracking on any individual unit without the need to come in contact with the participant/equipment. The OM500 can be remotely programmed to a variety of different transmission rate plans, as intensive as tracking at one (1) point per minute

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



and reporting the information every minute as well as a less intense plan that tracks one (1) point per minute and reports the information every ten (10) minutes. Other reporting intervals are also available based on agency preferences. **It is important to note that regardless of the reporting interval setting, alerts such as Tamperers and Exclusion Zone Violations are always reported immediately.**

Through the DNA monitoring system, our proposed solution provides the flexibility an agency needs for tracking these rate plans or levels of supervision each participant receives to meet individual monitoring needs. This level is defined by the type of monitoring assigned in the participant's equipment profile. The equipment profile not only defines the monitoring intensity but also allows the agency to change the level based on a participant's current monitoring status. It is important to know that at any time the rate plan can be changed to collect points more/less frequently and to report the information at differing intervals. It is also important to note that, **when in an Exclusion Zone or while in Pursuit Mode, the OM500 device increases its acquisition timers and collects location information every fifteen (15) seconds then reports the data to the web-based information system every thirty (30) seconds.** The most common profiles are identified below but may be customized to meet agency requirements as desired.

MONITORING PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point every one (1) minute and transmits data every ten (10) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every five (5) minutes. Tamperers and Zone Violations (Zones on Board) are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every one (1) minute and transmits data every thirty (30) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamperers and Zone Violations (Zones on Board) are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every one (1) minute and transmits data every sixty (60) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamperers and Zone Violations (Zones on Board) are immediately transmitted.	Lower risk participants requiring only standard supervision

—IMPORTANT SENTINEL ADVANTAGE—

For situations where officers are trying to pursue a GPS participant in real-time, our Pursuit Mode feature allows for the capture of a GPS location every fifteen (15) seconds with transmission of the points every thirty (30) seconds allowing for real-time tracking capability. This feature can be initiated by the Participating Entity officers, Sentinel personnel, or by our National Monitoring Center if requested by agency officers while in pursuit. Pursuit Mode tracking can be initiated from any internet accessible device through our web-based SentinelDNA monitoring system as well as from any mobile device through our DNA Mobile App.

SHADOWATCH (OPTIONAL)

The ShadoWatch wrist worn GPS device offers real time active GPS and passive GPS monitoring modes backed with the ability to download data in real time. Additionally, the ShadoWatch device is equipped with the latest and most up to date GPS chip sets and antennas, thus ensuring the most accurate GPS points

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



available. This includes the ability to track the time ("pings") to locate an individual to the minutes as well as the ability to "pinpoint" the distance and location to current industry standards. As it pertains to the time ("pings"), the accuracy of the GPS monitoring by default is a location point taken once every one minute. The devices can be set to receive/record location data up to as often as once every 10 seconds in cases where near real-time location information is required (i.e. pursuits, etc.). Information such as geo-address, date/time occurrence, speed of travel, number of satellites being utilized, etc. is displayed for each point received. In addition to GPS location, the technology utilized by our devices to pinpoint location accuracy such as through secondary location methods of Wi-Fi and LBS tracking, far exceed the industry standards of offender tracking. In Passive mode, the ShadoWatch can be set up to acquire a GPS point every one minute or every 5 minutes and report its data every hour.

- Tracking software must use Google maps, or similar, to monitor client movements.

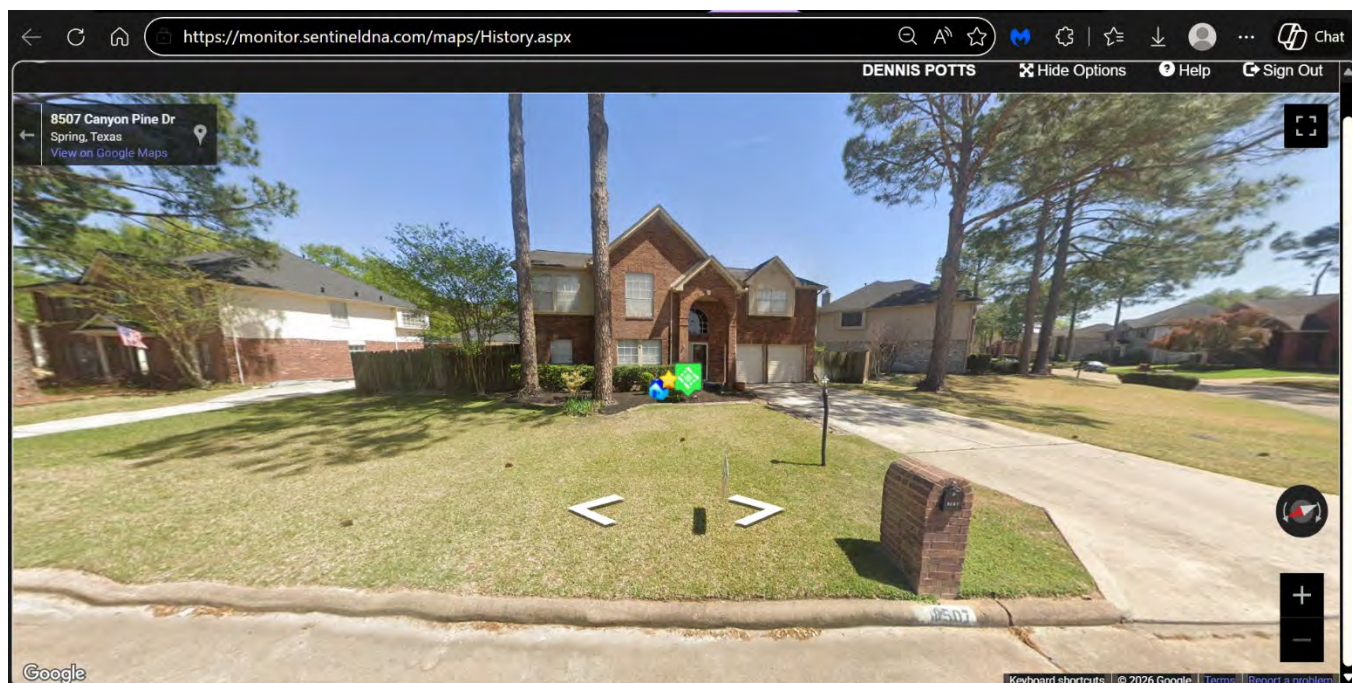
SENTINEL RESPONSE

OM500

Sentinel's DNA utilizes Google Maps® which provides automatic updates to the system always delivering the latest maps and upgrades. DNA tracks its own points and overlays the points on the most recent Google Maps® available at the time of 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). There are also multiple distinct views including traditional, bird's eye, and street view. These interactive maps contain easily recognizable images at the global level as well as down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking data on the map. With the click of the mouse button, DNA allows authorized users to "drill down" from a high-level view of a participant's overall tracking down to his/her tracking movements at a specific location.

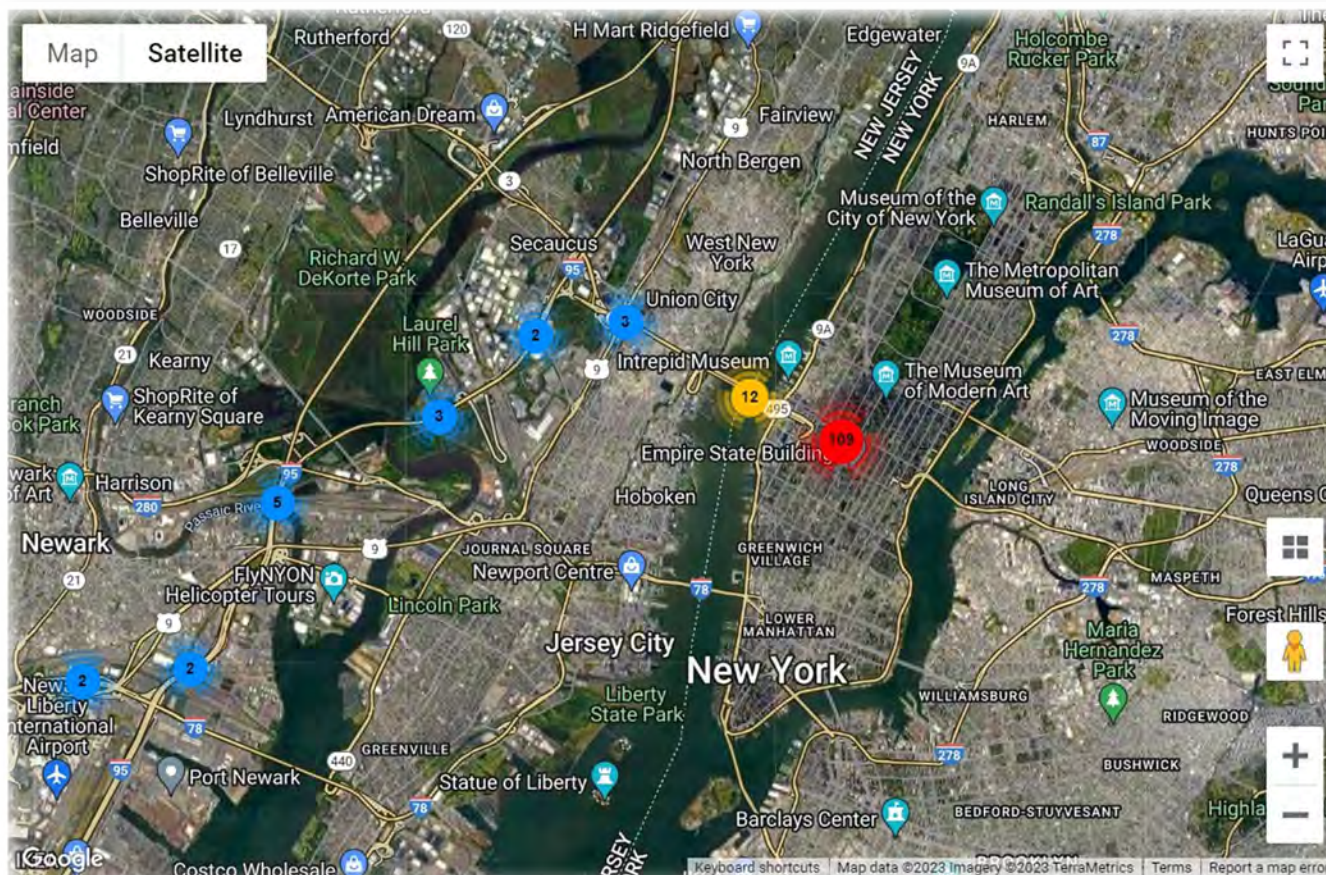
DNA STREET VIEW USING GOOGLE® MAPS





SHADOWATCH (OPTIONAL)

Tracking data is achieved through the ability of the ShadoWatch device to obtain location through GPS Satellite data and Wi-Fi data, as well as Location Base Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the devices are in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS nor Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located. Additional details such as battery percentage, speed of travel and direction of travel is also displayed. The mapping function allows the officer to filter tracking data by specific date and time periods and offers an automatic playback feature when reviewing tracking data. **Once again, reviewing tracking details on participants whether they are on GPS Tracking or App Related Services remains the same - thus making reviewing participant location data very simple.** Indicated on the next page are examples of the level of tracking detail obtained and displayed on Google Maps:



- Tracking software must have the ability to collect up to 30 days of location data and display it in an analytical view, allowing for easy dissemination of travel/stop patterns. Software must have the ability to apply analytics to:
 - Playback travel route taken by a client.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- Show stop locations and patterns.
- Create zones based on travel patterns.
- Show multiple clients shared locations.

SENTINEL RESPONSE

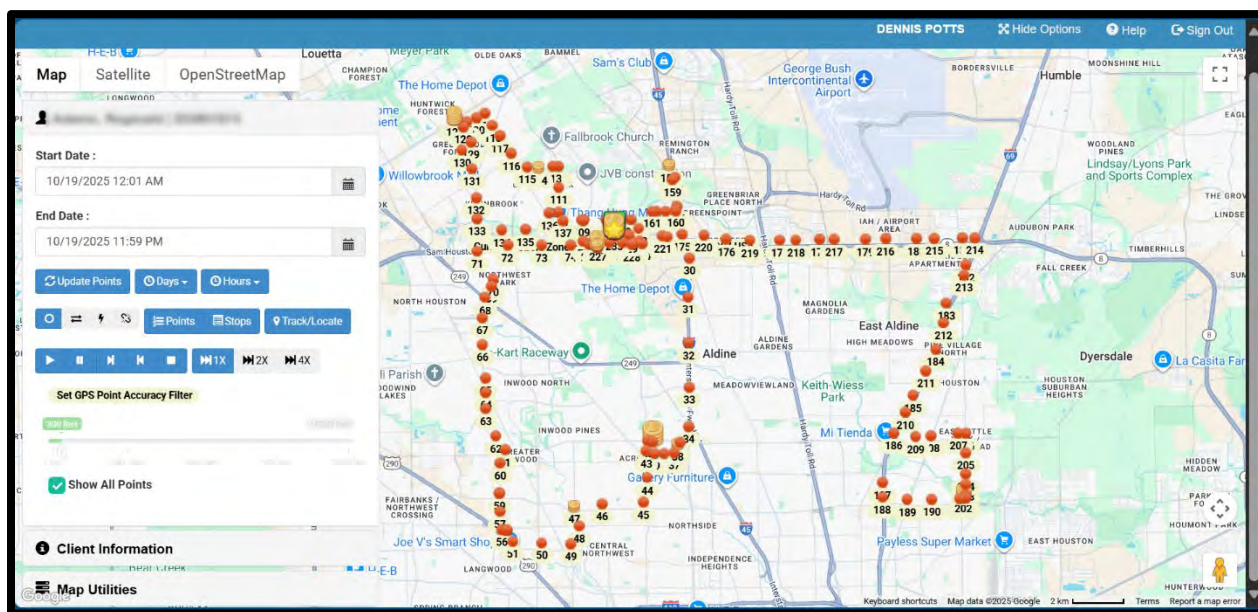
OM500

SentinelDNA collects and stores location data indefinitely and in accordance with Participating Entity storage requirements. While SentinelDNA can display 30 days in an analytical view, our customers have requested more detailed information breaking location data presentation into 24-hour increments. Should the need arise where a Participating Entity requests 30 days of information in an analytical view, Sentinel will comply and provide the requested data.

Playback Travel Route

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 participant’s overall tracking down to his/her tracking movements at a specific location. DNA also provides a point animation / DVD-style playback with fast-forward and rewind buttons. Tracking data is plotted on the map in numerical order of occurrence allowing for ease of viewing and during playback, the address, time of the location point, latitude and longitude of the location, and the speed at which the participant was traveling are all displayed beneath the playback controls.

DNA MAPPING UTILITIES SCREEN SHOWING CLIENT HISTORY / TRAVEL ROUTE



—IMPORTANT SENTINEL ADVANTAGE—

DNA provides additional reporting features for participants who are being tracked with GPS. From the Reports menu and the mapping screen, authorized users can run reports for a single participant or group of people:

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Stop Locations

The Points Report allows supervising entities to export all the participant's location data for the selected timeframe. The Stops Report allows supervising entities to export how long a participant was located within a geographical area; please refer to the example below. From the participant's location history page, select Points or Stops and select Add Report to Queue to generate the report.

- + **Points Report:** Displays the date and time, latitude, longitude, point type (GPS or Wi-Fi), and address for each point received during the time frame selected when viewing location history.
- + **Stops Report:** Displays how long a participant was located within a geographical area and includes the arrival date/time, departure date/time, duration, and address. Once the report is generated, it will only display those places where the participant was located for longer than the "Minimum Stop Duration in Minutes."
- + **Minimum Stop Duration in Minutes:** Defaults to 0. Enter a value to filter out locations on the Stops Report where the participant was present for less than a specific time duration, enter that time duration in minutes, and select "Add Report to Queue."



Report Time: Wednesday, April 5, 2025 1:23:48 PM PST

STOPS Report - Grid Size:100 - ID8708102 - Martinez, Dave

Time Interval: 3/1/2025 12:00:00 AM PST till 3/2/2025 12:00:00 AM PST

Arrival	Departure	Duration	Address
3/1/2025 12:00:48 AM	3/1/2025 6:12:53 AM	6 hr 12 min 5 sec	7210 Barrister Dr, Boise, ID 83704, USA
3/1/2025 7:08:00 AM	3/1/2025 7:12:54 AM	4 min 54 sec	11564 W Mount Hood Ave, Nampa, ID 83651, USA
3/1/2025 7:19:54 AM	3/1/2025 2:59:52 PM	7 hr 39 min 58 sec	12645 Ironstone Dr, Nampa, ID 83651, USA
3/1/2025 3:07:52 PM	3/1/2025 3:11:56 PM	4 min 4 sec	11564 W Mount Hood Ave, Nampa, ID 83651, USA
3/1/2025 3:18:55 PM	3/1/2025 4:39:57 PM	1 hr 21 min 2 sec	12645 Ironstone Dr, Nampa, ID 83651, USA
3/1/2025 4:52:57 PM	3/1/2025 5:06:54 PM	13 min 57 sec	218 2nd St S, Nampa, ID 83651, USA
3/1/2025 5:26:52 PM	3/1/2025 11:59:53 PM	6 hr 33 min 1 sec	7210 Barrister Dr, Boise, ID 83704, USA

Identifying Patterns and Multiple Clients Shared Location

Our Point Pattern Analysis (PPA) module within DNA provides automated detection/tracking of variances in participant movement patterns with both graphical and mapping views available to officers. Our Event Detection module identifies participants who were in the vicinity of an occurrence during a specific timeframe. By combining the Point Pattern Analysis and Event Detection modules within DNA, Sentinel is creating the ability to perform a search over a program's entire population database to determine if two (2) or more participants were within 25 meters of each other for at least one (1) minute. (Distance and time are configurable at the Participating Agency's request)

Point Pattern Analysis (PPA) is an automated analytics capability that enables users to quickly and easily identify changes in participant location/movement patterns that may be indicative of changes in behavior/compliance. To provide an agency with the most opportunities possible to create effective monitoring and in turn positive outcomes for participants, DNA includes Point Pattern Analysis (PPA) capabilities at no additional cost. This proprietary enhancement feature allows users to receive a comprehensive analysis of all their participants' routines.

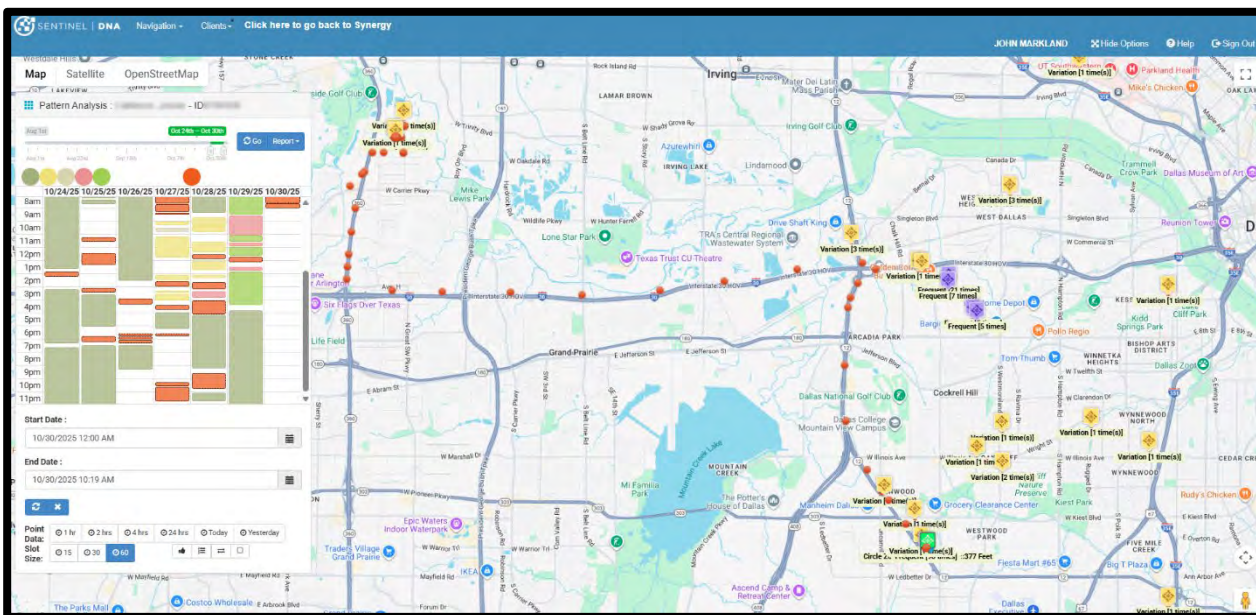
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Using our GPS point capture capability, our system can accurately track and display the participant's whereabouts 24/7. Although this is provided as part of the standard GPS tracking service, the advancements associated with PPA provide authorized users with a more in-depth review of a participant's tracking data. It will quickly identify "locations visited" by the participant and identify travel patterns. **PPA displays, in a detailed chart format, the periods of time when a participant was at a certain location.** The system is then 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 participant compared to variations that may be restricted locations.

Point Pattern Analysis examines locations frequented by each individual participant. 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-coding system, while locations that are new for the program participant are color coded in **RED**.



As an example, on the map display depicted above, a user can click on the locations and the position is displayed on a Google Maps 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.

Quick and Detailed Activity History: The system can track on an ongoing basis the data points previously visited by the participant to identify and display any new locations. This allows staff to quickly see the variations in the participant's movements across the community and verify where he/she is stopping throughout the day. This PPA feature is key to assuring that the participant is not straying from his/her required schedule.

For example, if the participant is only allowed to attend work, this system should display only two locations visited, his/her residence and his/her job site. It allows for identification of travel time, which also can be used by the officers or designated personnel to confirm that the participant is not loitering during transit times between these two (2) authorized locations.

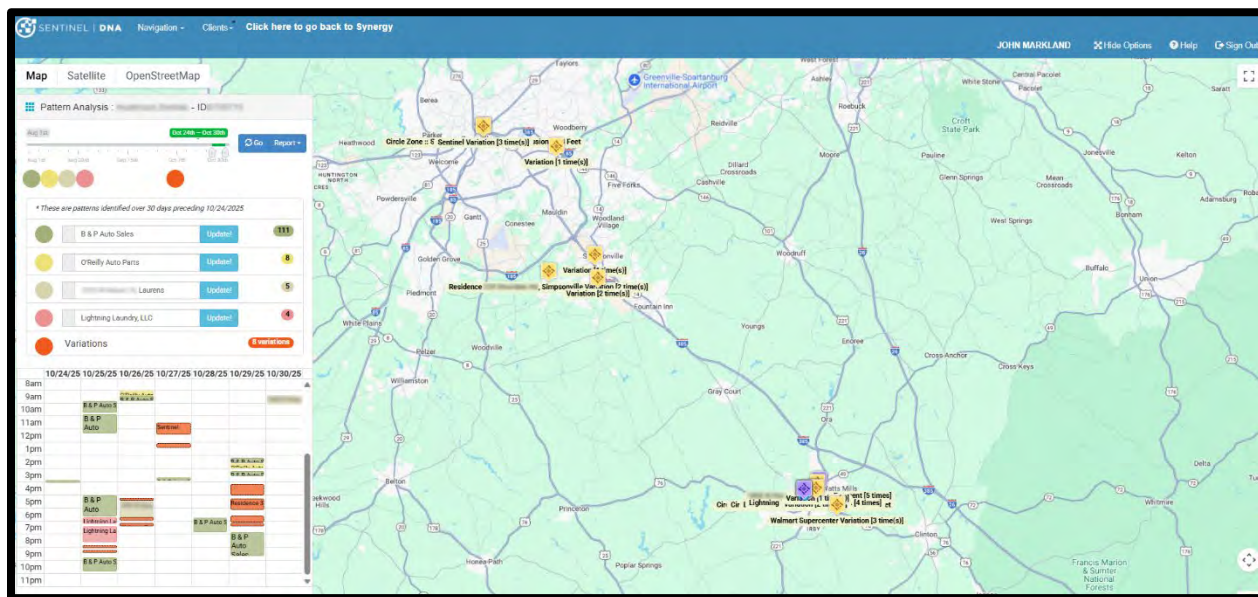
Authorized Location Identification: To make the analysis of a participant's activity easier, **DNA allows users to add labels to the authorized locations that a participant visits** as part of their daily, weekly, or monthly routine (e.g., home, work, church, counselor's office, etc.). Using these labels allows for the quick identification of a

Request for Proposals for ELECTRONIC MONITORING

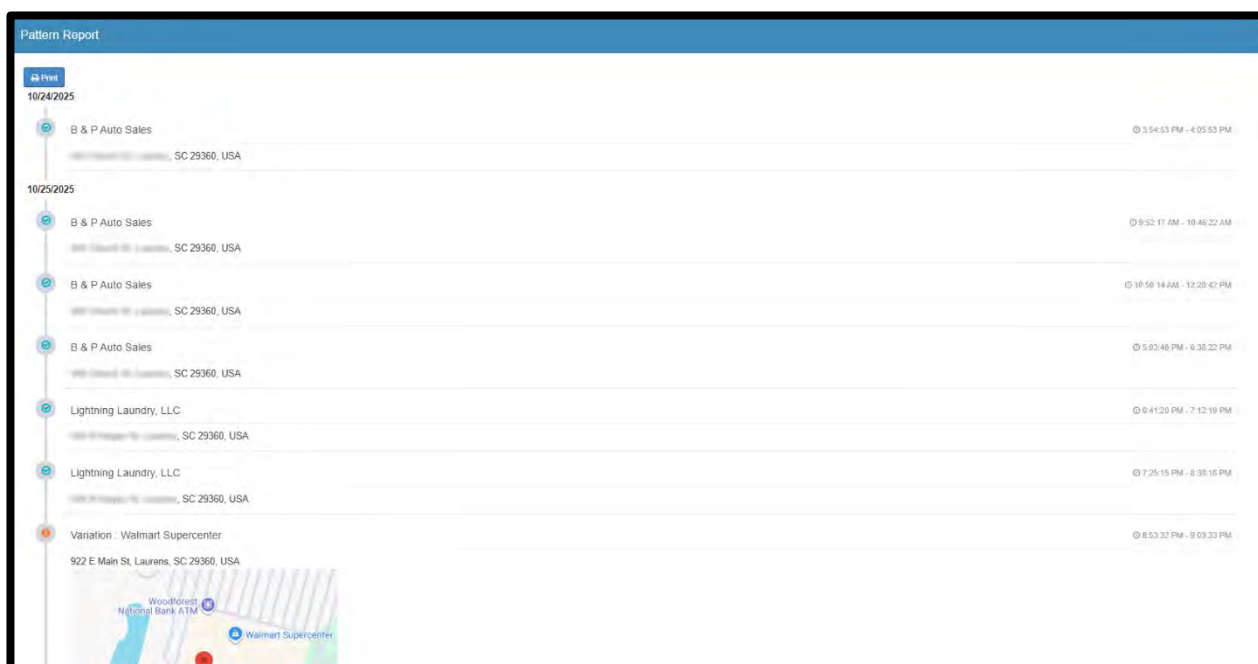
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



location that is not associated with a participant's given routine. The screenshot below illustrates how users can create custom labels to better identify locations frequented by a participant.



All data collected as a part of the PPA feature can be exported in a report form. The data will identify known locations based on the labels assigned to those locations as well as identify locations identified as variations using a street map view. Both known locations as well as variations are displayed within the report with the date and time of each event as shown in the image below.



Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



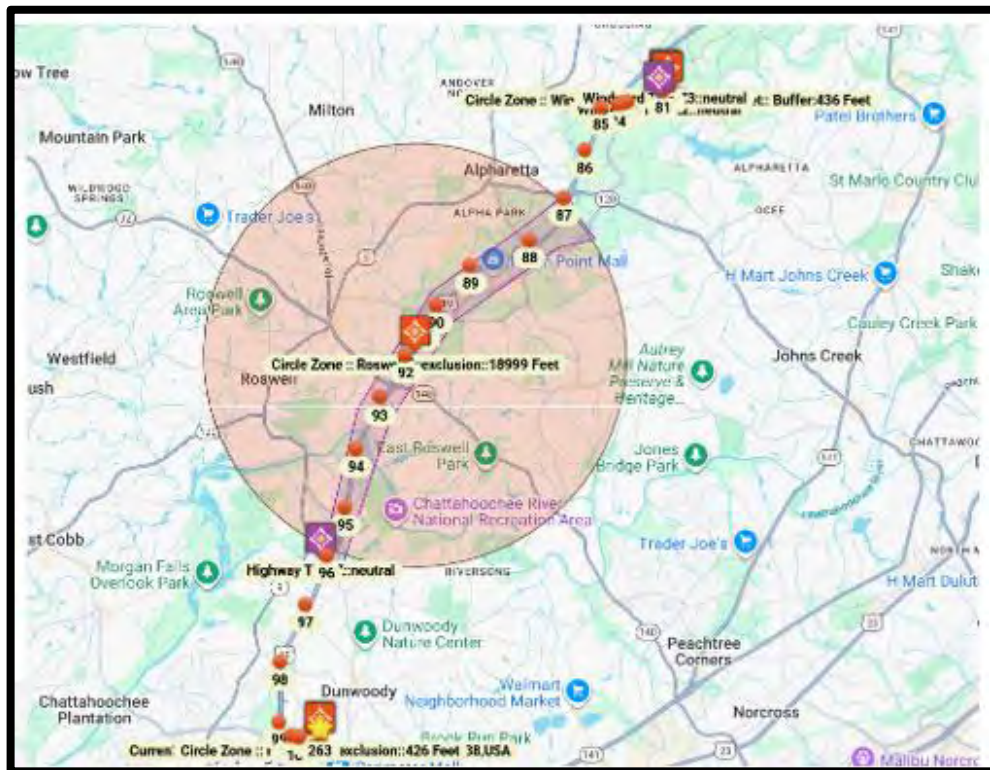
Create Zones Based On Travel Patterns

IMPORTANT SENTINEL ADVANTAGE—

Victim/participant separation is achieved using exclusion and buffer zones that create notifications on participant entry. However, use of these zones may impose impractical restrictions on participant travel; e.g., blocking a participant's ability to maintain employment, attend treatment or court sessions. With permission and when circumstances warrant, thoughtful application of **Neutral Zones** allows monitoring agencies to schedule limited **Travel Paths** into or through zones; i.e., exclusion zones, inclusion zones, and buffer zones.

The main function of neutral zones and travel paths is to prevent zone alerts when a device is within a designated "neutral zone" or "travel path" area during the allowed schedule time. When the neutral zone / travel path is active, buffer and exclusion zone alerts will be suppressed, and enter/exit events are only recorded for the neutral zone unless the participant deviates from the neutral zone or travel path. Please note that if a device enters an area covered by an overlapping buffer or exclusion zone outside of the neutral zone schedule or travel path, alerts for those zones will be triggered as usual. The following scenario illustrates how neutral zones and travel paths function in practice.

Travel Path Overlapping Large Exclusion Zone: The issue presented is that a client's work location requires the client to pass through a buffer/exclusion zone; as shown in the image below, the client must travel down a main highway to reach their place of employment, however a large exclusion zone covers the highway. The solution is to **create a neutral zone schedule as a travel path** to allow the participant to travel through the zone at pre-set specific times when the neutral zone takes priority, as depicted in the following screen shot.



Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



—IMPORTANT SENTINEL ADVANTAGES—

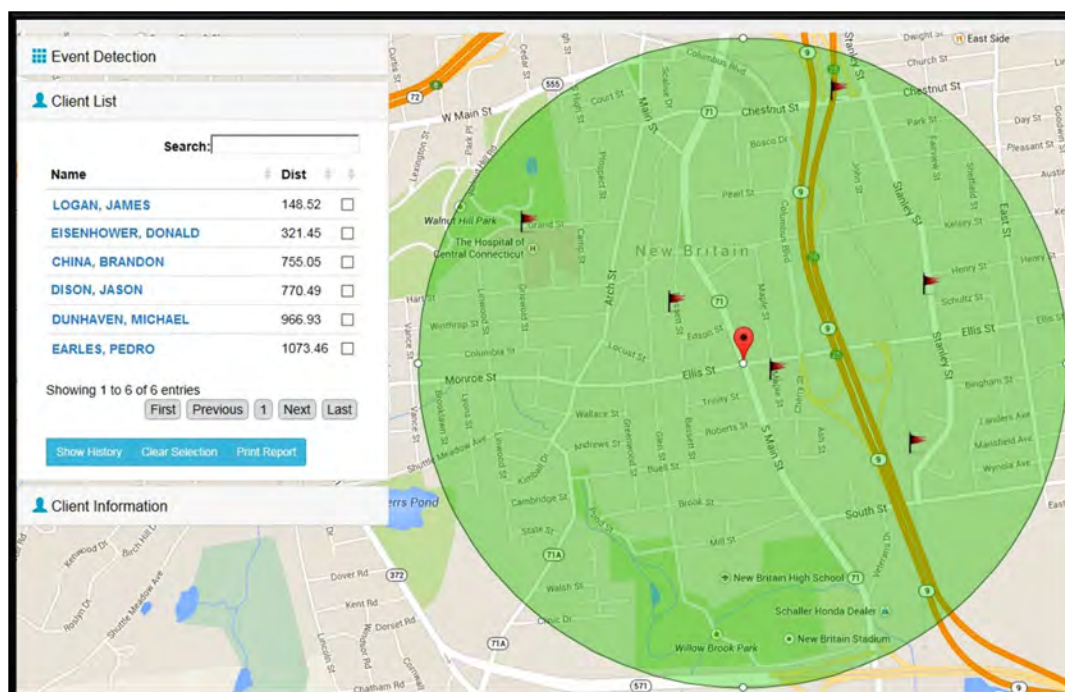
- + **Entering Travel Path Outside Schedule:** If a Neutral Zone has a schedule (e.g., 7 am to 8 am) and the device enters the travel zone after the schedule ends (e.g., after 8 am), alerts will be raised for the Exclusion zone.
- + **Deviating from Neutral travel Path:** If a client travels through a Neutral Zone travel path overlapping Buffer and Exclusion zones during the allowed schedule time but deviates from the Neutral path, alerts will be raised as expected for the first point plotted outside the Travel Path and within the exclusion zone.

Show Multiple Clients In Shared Location:

Sentinel's **DNA Event Detection (Crime Scene Correlation)** feature within DNA has a mapping component that correlates crime and/or incident report data collected from local law enforcement agency stakeholders and associates the data with the tracking data of participants.

Our Event Detection mapping feature will identify participants who were in a specified vicinity of an incident address during a specific date/time range. Event Detection will simultaneously provide information for participants who are in the vicinity at the date/time of occurrence of the crime. Once the data has been entered, and the search has completed, the system will provide a Participant List and place a flag on the map for each participant in the results list and represent the location of the participant that was closest to the search address during the time frame selected.

The search results are displayed under a precise "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 address radius within the time frame selected, thereby creating a list of potential individuals for law enforcement follow up. The system also displays the participant's actual distance from the address of interest, as shown below. Furthermore, all other GPS participants can be eliminated as potential individuals as they were not in the vicinity at the date/time in question.



Request for Proposals for ELECTRONIC MONITORING

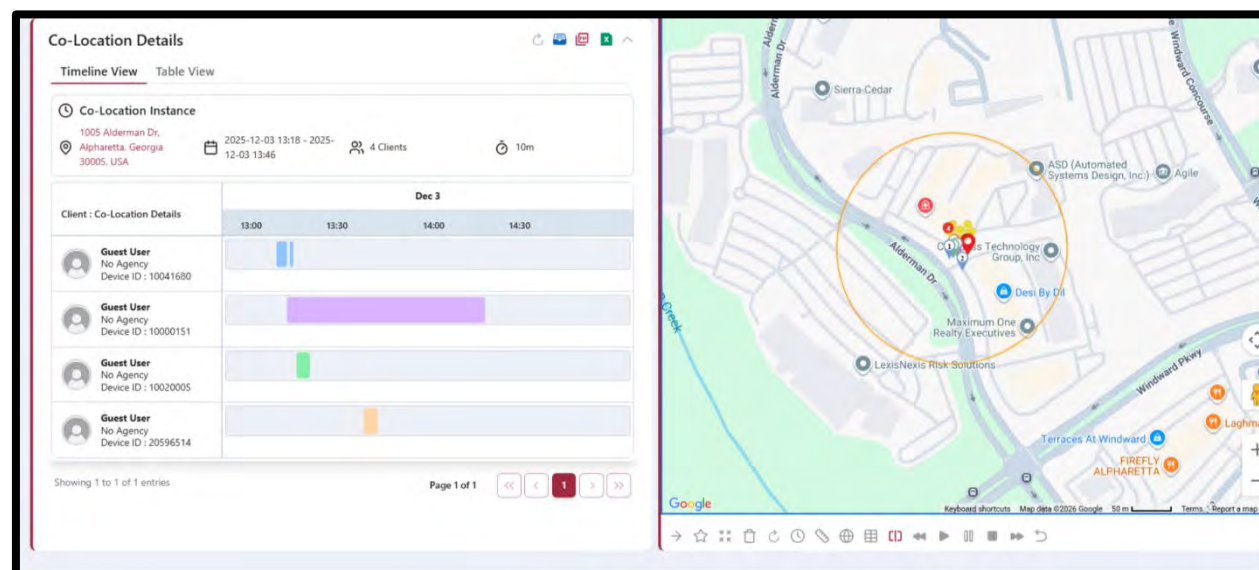
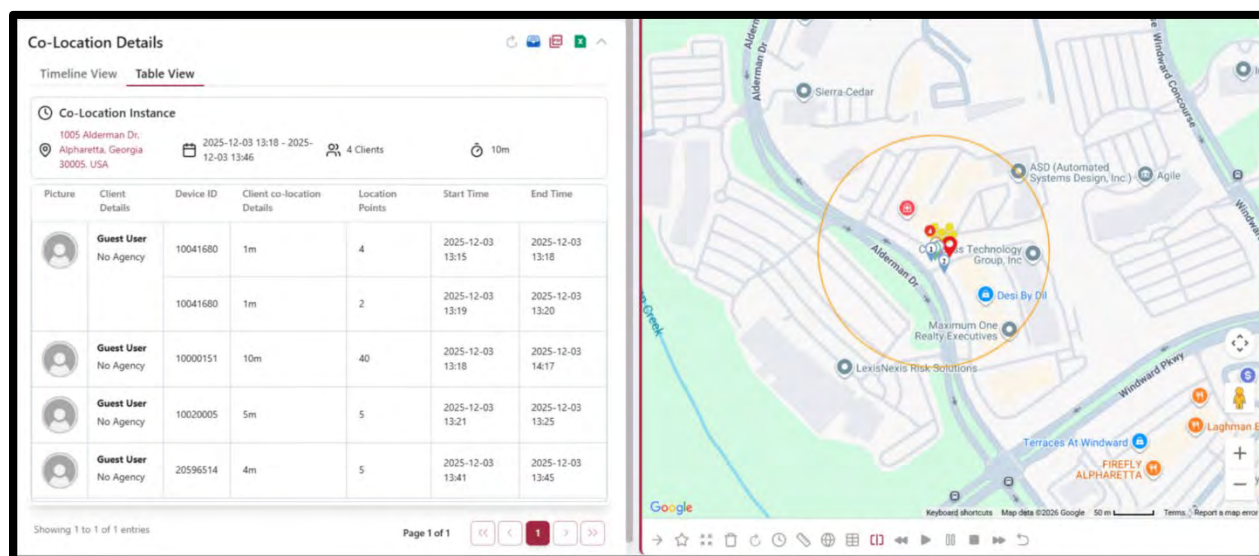
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



In addition to our ability to track multiple clients through our Event Detection Module, Sentinel is in the final stages of releasing our Co-location module within SentinelDNA with release scheduled for Q2-2026. **Co-Location is an automated analytics capability that enables users to efficiently identify instances in which multiple GPS participants were present at the same location at the same time, or at the same location at different times. Identified co-location instances will be presented through graphical, map-based, and tabular data views. These patterns may indicate potential changes in participant behavior or compliance.**

This tool will allow officers to analyze the behaviors / daily routines of several clients at one time to determine if the participants are co-locating and quickly identify deviations that may indicate a compliance issue. This tool will also aid officers who are tasked with tracking gang and criminal behaviors as the module will allow officers to view on a map all the participants who are potentially interacting with known criminals as well as the locations of where the participants choose to meet and/or congregate.

Below is a screen image of the upcoming **Co-Location Module** showing how several groups within the demonstration program have co-located – including the map as well as start / stop times.



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



While the Co-Location Module is currently in development and will be available to our customers in Q2-2026 Sentinel will provide updates on the progress and development status for the Module and include it within our Analytics offering upon completion.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE tracking software has the ability to collect up to 30 days of location data and display it in an analytical view, allowing for easy dissemination of travel/stop patterns. The ShadowtrackONE software has the ability to apply analytics to:

- + Playback travel route taken by a client.
- + Show stop locations and patterns.
- + Create zones based on travel patterns.
- + Show multiple clients shared locations.

Tracking Detail with Google Maps

Tracking data is achieved through the ShadoWatch devices' ability to obtain location through GPS Satellite data and Wi-Fi data, as well as Location Base Services (LBS) that overlay the tracking points on Google Maps. Each location point contains the latitude/longitude, and the system automatically translates and geocodes this data into a precise address where the participant is located on Google Maps. Additional details such as battery percentage, speed of travel and direction of travel are also displayed. The mapping function allows the officer to filter tracking data by specific date and time periods and offers an automatic playback feature when reviewing tracking data. Once again, reviewing tracking details on participants whether they are on GPS Tracking or App Related Services remains the same using Google Maps - thus making reviewing participant location data very simple, as shown on the below images.



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Date Range
Custom

Filter Start (User Time)
12/10/2023 2:00 PM

Filter Start (Enrollee Time)
12/10/2023, 2:00 PM

Export

Filter End (User Time)
12/10/2023 5:00 PM

Filter End (Enrollee Time)
12/10/2023, 5:00 PM

Maximum 250 locations displayed

1 to 5 of 173

1	12/10/2023 04:59 PM EST	Address	GPS Speed: 38.66	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
2	12/10/2023 04:57 PM EST	Address	GPS Speed: 37.48	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
3	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
4	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
5	12/10/2023 04:55 PM EST	Address	GPS Speed: 33.37	Battery: 81 Charging: No Signal Strength: 66 Zone Status:

Inclusion/Exclusion Zones

Agency staff can easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones are automatically created around the borders of the desired States or Counties. Zones can be created specifically for an individual enrollee or shared between multiple participants.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SAMPLE CIRCLE ZONES

Shadowtrack | McAndrew, Tom (Shadowtrack) Search enrollments, entities & users

Zone Name: Massachusetts Probation

Default Location: Yes ☒ No

Exclusion: Yes ☒ No

Beacon: Yes ☒ No

Street: 1 Ashburton Place

Unit: Room 405

City: Boston

State: MA

Zip Code: 02108

Country: United States

Find Location

Center: (42.3599412629689, -71.0623880052851)

Radius (ft): 374.06

MAC Address

Save Cancel

SAMPLE POLYGON ZONES

Shadowtrack | McAndrew, Tom (Shadowtrack) Search enrollments, entities & users

If you want to edit the coordinates of an existing polygon, click it to enable edit mode.

Zone Name: Massachusetts

Default Location: Yes ☒ No

Exclusion: Yes ☒ No

Beacon: Yes ☒ No

State-wide: Massachusetts

County

MAC Address

Save Cancel

- Must have a method of p Priority e Communication, or similar feature, of location data on a wireless network to ensure continuous communication of location points in high traffic times and critical situations. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

OM500

The OM500 device ensures continuous communication of location data by prioritizing GPS satellite tracking and automatically transitioning to alternative location methods when GPS data is unavailable. Location points are first obtained via GPS satellites based on the device's rate plan. If GPS points cannot be obtained, the device automatically switches to Wi-Fi-based location data, and if neither GPS nor Wi-Fi is available, cellular cell-tower



scan location points are generated. Location data is processed through a third-party provider to determine position and accuracy, ensuring uninterrupted location reporting during high-traffic periods and critical situations.

The OM500 is the most advanced one-piece GPS Offender Tracking and Location Monitoring unit in the industry that reliably communicates monitoring and location data over the Verizon LTE or AT&T LTE networks including all roaming partners. To ensure continuous communication of location points in high traffic times and critical situations, the OM500 supports, and Sentinel is approved for, activation for its OM500 GPS devices on Verizon's Frontline network that prioritizes communications and delivers enhanced connectivity during high traffic times and critical situations. With this approved capability from Verizon, the OM500 is equipped to provide NASPO ValuePoint Participating Entities continued and reliable communications during critical situations and emergency conditions. With tens of thousands of devices communicating daily Sentinel has not seen nor been subject to high traffic delays even during critical situations such as hurricanes or fires.

Further, the OM500 device incorporates advanced technologies and methods to ensure that tracking and location monitoring points from an entity program participant wearing an OM500 device accurately and continuously reports location data, through the following advance technological methods.

- + **Zones On Board.** The OM500 incorporates smart device technology that allows for GPS-based **zones "on board"** whereby, the device will immediately report zone violations and tamper alerts immediately in high traffic times and critical situations. This method is far superior to other providers who store zones on the monitoring application and cannot immediately report key alerts.
- + **Pursuit Tracking Mode.** For situations where officers are trying to pursue a GPS participant in real-time, our Pursuit Mode feature allows for the capture of a GPS location every fifteen (15) seconds and report every (30) seconds allowing for real-time tracking capability. This feature can be initiated by Department officers, Sentinel personnel, or by our National Monitoring Center if requested by Department officers while in pursuit. Pursuit Mode tracking can be initiated from any internet accessible device through our web-based Sentinel monitoring system as well as from any mobile device through our Mobile App.
- + **Industry Leading Triple Tracking Capability via GPS, Wi-Fi location Points, and Cellular Tracking.** The OM500 leverages three (3) industry-leading location-based services provided by Skyhook. This hybrid Precision Location system locates our devices using GPS, Wi-Fi and cell signals ensuring that all devices can be accurately located in virtually every environment, including high traffic times and critical situations. In impaired areas where GPS alone cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. **This allows for a significantly more robust device as it offers multiple tracking options.**
- + **Triple Tamper Detection including: 1) fiber-optic strap design strap tamper; 2) device case tamper; and 3) backplate tamper.** Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and dual pressure sensors within the device, *the OM500 device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tampers with the strap.* The OM500 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate, indicative that the device has been uninstalled/disassembled. Additionally, the unit will send a tamper alert if the unit is broken/cracked or if the unit's backplate is separated from the rest of the device.

The above advanced features ensure continuous communication of location points in high traffic and critical situations.



SHADOWATCH (OPTIONAL)

The ShadoWatch provides continuous location monitoring of designated low to moderate risk program participants through the use of an attractive tamperproof wristwatch, with color display and, is managed through the ShadowtrackONE monitoring platform. The ShadoWatch incorporates Wi-Fi, GPS and Location Based Services (LBS) technology to increase location accuracy while enhancing battery life. In addition, an officer can communicate through the watch directly with the participant by using two-way voice, individual or mass electronic messaging. To ensure connectivity during high traffic times, the ShadoWatch is equipped with enhanced Antennas that support AT&T and T-Mobile 4G LTE, GPS & WIFI based technologies and communicate using multiple cellular network providers and automatically switch between providers and their respective roaming partners' cellular networks based on service availability. This approach ensures that if one network were to fail, be unavailable, or degraded, the ShadoWatch devices would automatically fail over to other operating networks.

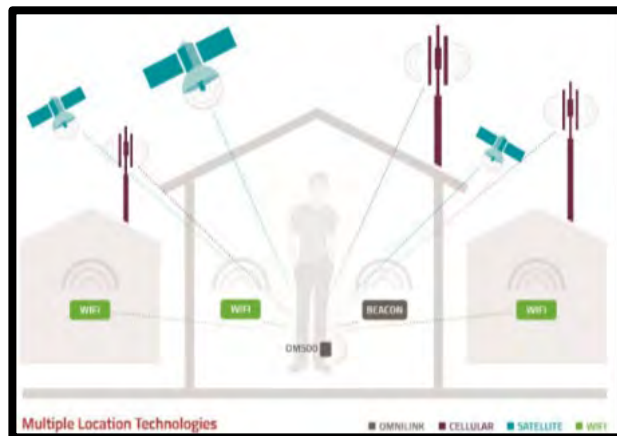


- Optional Wi-Fi tracking, in addition to cellular, to ensure tracking is not lost when GPS points are unavailable.

SENTINEL RESPONSE

OM500

The OM500 is equipped with three (3) location technologies to ensure that program participants are continually tracked, even in the absence of satellite signals. **The OM500 uses GPS, Cellular, and Wi-Fi technologies to track program participants' locations.** This triple-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the OM500 will automatically switch to cellular tracking and Wi-Fi technologies to continue tracking the participant. Wi-Fi location points are generated using precision location services from Skyhook and the OM500 device will switch to Wi-Fi points when the device is unable to obtain GPS points.



The OM500 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM500's unique design combines these multiple layers of location technologies whereby the device does not have to connect to the Wi-Fi signal, and the signal only needs to be visible to the device. In conditions where GPS and Wi-Fi are not available, the device will automatically switch to cellular tracking location points generated when the device can see one or more cell towers and the location of the point is calculated based on the strength of each visible tower with respect to the location of the device. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The combination of these advanced location technologies allows for the quickest acquisition time without being required to go outside to acquire a GPS signal when enrolling and installing a device.



SHADOWATCH (OPTIONAL)

The ShadoWatch provides continuous location monitoring of designated low to moderate risk program participants through the use of a tamperproof wristwatch, with color display and, is managed through the ShadowtrackONE monitoring platform. The ShadoWatch incorporates GPS, Wi-Fi, and Location Based Services (LBS) technology to increase location accuracy while enhancing battery life.

- Must have the ability to configure state, county, and school zones, and allow for additional unlimited zone creation. Must have points of exclusions (parks, schools) alerts for when device enters one of those points.

SENTINEL RESPONSE

OM500

SentinelDNA allows for the ability to configure state, county, and school zones as well as allowing for additional unlimited zone creation. Authorized users will have access to create, edit, and delete exclusion and inclusion zones for participants being tracked via the GPS tracking device. **SentinelDNA allows for a virtually unlimited amount of exclusion and inclusion zones per participant.** For participants with challenging zones, DNA is also configured to support construction of customizable 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 monitor the movement of the individual program participants.**

Zones can be created as an individual zone, if only one participant will need to use the zone, or as a template zone that can be created and stored within the system as a library of zones if there are multiple participants who need to use the same zone. **These zones are used to identify and alert on locations such as parks, schools, known gang locations, bus terminals, airports, etc. DNA allows for the creation of template zones that can be used across a specific population of participants.** This allows agency personnel to designate certain sites across a region as exclusion zones for an entire population of multiple participants. This eliminates the need to repeatedly re-create the same zones for all the individuals identified in a specific population. This type of **template zone** set-up can be used for sex offenders and other high-risk participant populations establishing zones around schools, playgrounds, or related areas of concern.

—IMPORTANT SENTINEL ADVANTAGE—

In addition to the ability to create individual **Inclusion and Exclusion zones in the shapes of circles, rectangles, and arbitrarily shaped polygons, as well as being able to have zones within zones**, Sentinel's DNA web-based system will also allow the agency to create / establish **advanced warning parameters by including buffer zones around exclusion zones** to alert individuals of an upcoming potential violation of the zone. DNA also allows agencies to utilize mobile exclusion zones in addition to stationary exclusion zones.

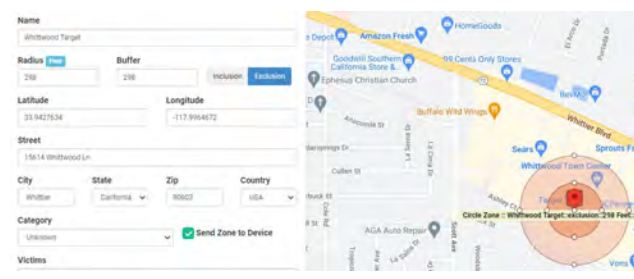
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



GPS Buffer Zones: Buffer zones provide an extra layer of notification around exclusion zone borders and **enhance notifications to allow for a 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. This places 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 buffer and exclusion zone area.

EXAMPLES OF MOBILE EXCLUSION ZONE AND
BUFFER ZONE IN DNA



Mobile Exclusion Zones (MEZ): Mobile Exclusion Zones (MEZ) allow agencies to track if a participant on GPS monitoring comes near another specific individual anywhere, they may be in the community. Often used for victim notification applications and in domestic violence cases, the victim has a zone which is created around their smartphone while the perpetrator/participant wears an OM500 GPS tracking device.

Sentinel incorporates the use of the MEZ format through our **Advocate™, Victim Notification and Tracking Application**, which enables the configuration of the Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilizes the victim's smartphone to acquire and report GPS data to our DNA monitoring system. Advanced GPS monitoring technology tracks the location of both the offender and the victim. If the OM500 device comes within an agency specified distance of the victim's smartphone, the victim receives notification on their smartphone of the Mobile Exclusion Zone breach giving her/him necessary information to help initiate her/his safety plan. Additionally, law enforcement may be contacted at the discretion of the Agency.

The Sentinel offender/victim tracking solution gives officers the ability to continuously monitor an offender's proximity to their victims. The locations of the offender and the victim are recorded as historical data giving officers insight into how much time an offender is spending in the vicinity of a victim. The size of the Mobile Exclusion Zone is determined by court order or the agency and may range from hundreds of feet to hundreds of miles. The Mobile Exclusion Zone also incorporates the use of a Buffer Zone in order to create an extra layer of notification and enhance the agency's tracking capabilities when utilizing the Advocate Victim Notification and Tracking Application.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application has the ability for users to create inclusion and exclusion zones as circles or hand drawn polygon shapes allowing staff to easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones can be automatically created around the borders of the desired States or Counties. Additionally, Zones can be created specifically for an individual participant or shared between multiple participants. Once the zone is created, time schedules/restrictions can be easily assigned through the scheduling feature.

Zones can be set up to ensure that the participant is in the authorized area(s) at all times. Any compliance deviations can be immediately reported to supervising staff and notifications can be immediately generated. Notifications can be delivered via an SMS text message, email, and/or via an automated voice call to desired phone number(s). Additionally, field supervising staff can utilize Shadowtrack's Officer Mobile App and/or staff can utilize our desktop web-based monitoring software to monitor the participants in real-time.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Inclusion/Exclusion Zones

Agency staff can easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones are automatically created around the borders of the desired States or Counties. Zones can be created specifically for an individual participant or shared between multiple participants.

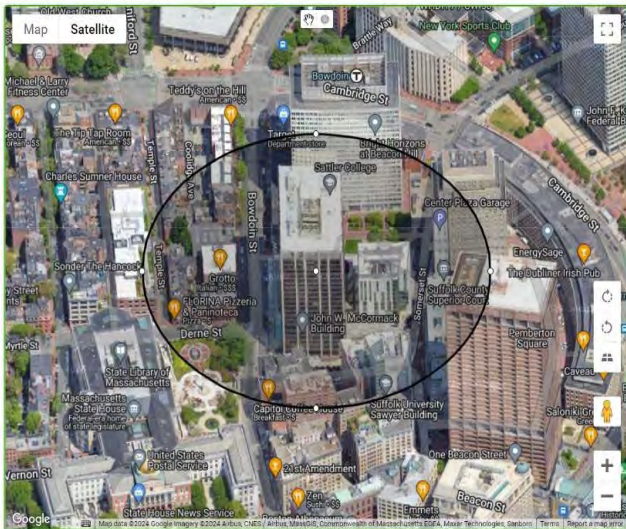
shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack|McAndrew, Tom (Shadowtrack)

Search enrollees, entities & users

Map Satellite



Zone Name

Massachusetts Probation

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

Street

1 Ashburton Place

Unit

Room 405

City

Boston

State

MA

Zip Code

02108

Country

United States

Find Location

Center

(42.35990412639689, -71.0623588005265)

Radius (ft)

374.06

MAC Address

Save

Cancel

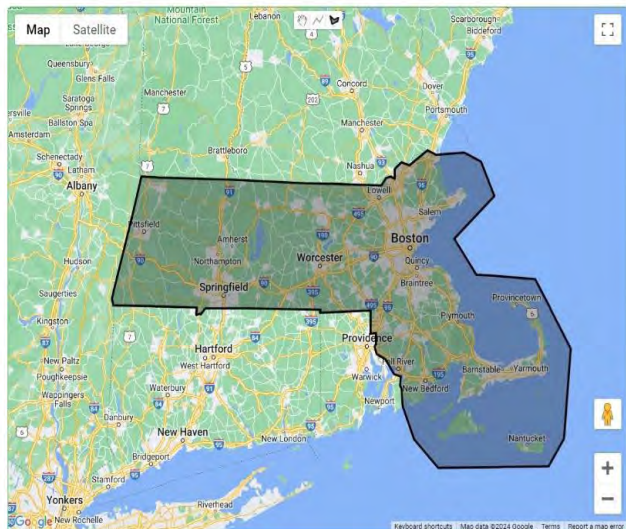
shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack|McAndrew, Tom (Shadowtrack)

Search enrollees, entities & users

Map Satellite



Zone Name

Massachusetts

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

State-wide

Massachusetts

County

MAC Address

Save

Cancel



- The system must provide the capability for Participating Entity to download data and reports from the database, through secured internet access.

SENTINEL RESPONSE

OM500

SentinelDNA will provide the Participating Entity secure internet access to system data and reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system. **Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement.** Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA REPORT MENU SCREEN

A screenshot of the Sentinel DNA Report Menu screen. The interface has a blue header with the Sentinel logo and a navigation bar. On the left is a sidebar menu with options like Dashboard, Agency, Reports, Basic Reports, Supervisor Reports, Enrollment, Maps, Operators, Inventory, Management, and Administration. The main area is titled "Report Menu" and contains a "Reports" section with a list of report types such as "Client All Activity", "Enrollment Report", "Deletion Report", "Group All Activity", "Client Alarm Totals - Active Alarms", "Client Alarm Totals - Short", "Active Client Report", "Count Current", "List Of All Away Clients", "Event Detection", "More reports", and "Equipment reports". On the right is a "Parameters" section with fields for "Clients", "From Date" (08/03/2025), "To Date" (08/04/2025), and checkboxes for "Posted Time", "Event Time", and "Suppress BART Check". A "Submit" button is at the bottom right.

If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE monitoring application has a wide array of report options ranging from violation reports to inventory control that can be downloaded, printed, and/or exported in various formats (PDF, Excel, etc.). From within our monitoring platform, agency personnel can easily review/download/print/export the activity of a single participant or generate additional reports specific to the agency needs. Many of the reports already available were requested by current customers. If the agency is in need of additional reports, our customer service and software development teams will work together to get anything else that may be needed or requested by the agency at no additional cost.

An example of a list of reports currently used by customers for the ShadoWatch include the following reports:

- + Alarms report
- + Charging History Report
- + Locations Report
- + Visit Points Report

Visit Points are generated in the system based on the following:

- + Minimum of 2 location points
- + Within a 3-minute period
- + Within a 50m radius

The Visit Points Report has been described by current agency users as being very helpful as it gives details including specific locations arrival time, departure time, duration (in minutes), the location address, and the latitude and longitude.



- The system must provide the functionality and access required with 99.99~~999~~% uptime/availability avoiding any downtime due to hardware or software issues. This will include a continuity of operations plan and disaster recovery plan which will ensure the system and services will be available without disruption as required. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

OM500

Sentinel is committed to providing a highly available system and can formally commit to a 99.99% uptime availability target. The system is designed with reliability and operational monitoring controls to minimize service disruptions due to hardware or software issues. Sentinel will provide a copy of our Continuity of Operations Plan/Disaster Recovery Plan upon request.

SHADOWWATCH (OPTIONAL)

Shadowtrack's web-based software, ShadowtrackONE, is a mission critical element of the electronic monitoring system. As such, Shadowtrack has redundant instantiations of the system. If the primary software platform were to have an outage the backup platform can be engaged within minutes to prevent any prolonged system outage. This failover is periodically tested to ensure proper functionality. Data Center Electrical or Internet Connectivity Outage. Shadowtrack partners with Amazon Web Services (AWS), with servers located in different regions of the United States. Shadowtrack's activity is cloud-based, and access to the case management system or any of the raw data requires two-factor passcode identification and authorization along with other security measures. Operating with various locations worldwide, Shadowtrack accepts and follows each agency's data and information record retention requirements. The systems are monitored 24/7/365; augmenting Shadowtrack's IT team in ensuring that the physical environment is both stable and secure and achieves uptimes required by this RFP.

C. GPS Customer Support & Training

C. Customer Support and Training:

- The Contractor must provide a dedicated account representative.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

As a leading provider of electronic monitoring services and as a NASPO ValuePoint contractor for more than 25 years, Sentinel has established processes and protocols to effectively deliver services via NASPO ValuePoint agreements. Sentinel will continue to ensure familiarity with the Master Agreement including all terms and pricing.

The NASPO ValuePoint Agreement will receive full attention of Sentinel's Senior Leadership team as evidenced by the fact Sentinel is appointing Mr. Mike Dean, Sentinel's Senior Vice President of Sales as the point of contact for the NASPO ValuePoint Master Agreement.

MIKE DEAN | Senior Vice President of Sales

- + Mr. Dean oversees all Sentinel sales personnel and manages the company's cooperative purchasing agreements. With over 33 years in the electronic monitoring industry overseeing sales and contracting for some of the largest electronic monitoring providers, including BI Incorporated, 11 years, G4S Justice Services, 7 years, and Sentinel for the past 14 years, Mr. Dean has unparalleled expertise in



collaborating with Federal, State, and Local Governments, developing electronic monitoring programs and leveraging cooperative purchasing to the benefit and convenience of government agencies.

- + Mr. Dean has worked directly with procurement departments negotiating Participating Addendums and reviewing contractual requirements for entities that makes him an exceptional subject matter expert and primary point of contact for the NASPO ValuePoint Cooperative Purchasing Agreement. Mr. Dean holds a Bachelor Agreement in Criminal Justice, from the University of Cincinnati, and as Senior Vice President of Sales, Mr. Dean is strategically positioned to champion the NASPO ValuePoint agreement. He will provide oversight for the NASPO ValuePoint Master Agreement and for the agency's participating addendums, programs and purchasing department, while also facilitating all post-award implementation adjustments required for this contract.

Mr. Dean will work closely with the Sentinel Field Operations Team and have complete support from our Chief Operating Officer, Mr. Darryl Martin. Mr. Martin has been overseeing the delivery of electronic monitoring services to the NASPO ValuePoint Agreements for more than 25 years. Mr. Martin will exercise all Sentinel departments and employee base of more than 280 to ensure complete compliance with the Master Agreement including the following resources that stand ready to continue providing services.

Mrs. Melissa Staff, Sentinel's Senior Vice President of Field Operations, is responsible for the management and oversight of our Regional Account Management team as well as Sentinel's national network of customer support and branch office personnel. Her team manages the day-to-day needs of our benchmark offender-funded programs as well as providing customer service to our agency-funded contracts across the United States. **A dedicated account representative will be assigned to each Participating Agency for the duration of contract operations.** The Sentinel account representative will be responsible for:

- + Account retention;
- + Being the main liaison between the Customer and Sentinel;
- + Providing consultative account management practices to government channel accounts in their region to ensure best practices are in place;
- + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
- + Introduction and socialization of hardware and software offerings that may benefit the Customer;
- + Conducting training and overseeing the implementation; and
- + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.

- The Contractor must provide support functions 24/7/365, via phone call, email, and help desk.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained technicians and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

Our monitoring centers are staffed 24 hours a day, 7 days a week with live staff including a supervisor always on duty and certified operators cross-trained to support our suite of supervision services and monitoring products. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.



—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year. **There is no subcontracting of any of our proposed monitoring services.**

Sentinel provides access to designated **Help Desk** staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. Sentinel provides toll-free telephone access, toll-free fax line, and email access to over 60 operators and customer service representatives, available to officers 24 hours a day, 7 days a week, 365 days a year, who can resolve most technical problems over the telephone or through remote diagnostics.

Sentinel strives to resolve all customer inquiries promptly and on first contact. Each monitoring center operator has the expertise to easily identify, explain, and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert and changing a participant's schedule.

- The Contractor must provide toll free access to customer support/monitoring center.

SENTINEL RESPONSE

As stated above, Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained operators and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

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

In the unlikely event that problem solving requires a higher-level of involvement, Sentinel's customer service is equipped with all necessary computer equipment and staffed by experienced technicians, as well as the engineers who developed the system technology, who can quickly analyze and resolve the problem.

- The Contractor must provide initial start-up training that must include but not be limited to the following:
 - o The enrollment of clients into the software system.
 - o The installation, use, de-installation, and cleaning of the equipment.
 - o The generation and interpretation of data/monitoring reports.
 - o Accessing/using Contractor's technical support/help menus and monitoring center.

SENTINEL RESPONSE

Sentinel understands that training and customer service are crucial to the success of any electronic monitoring program, and Sentinel is dedicated to meeting those needs. Sentinel agrees to provide the initial training session and ongoing training, including all manuals, concerning the implementation and management of the monitoring



program as determined by the contract. Sentinel is committed to establishing a partnership over the term of the contract to ensure that all staff members are fully and properly trained. Training is offered for the life of the program as outlined in the monitoring services agreement at no additional cost.

Sentinel's training philosophy for our instructor-led courses can be a combination of respondent training as well as train-the-trainer if so desired by the Participating Entity. We work to provide all training for our customers based on their individual programmatic needs and thus will work with the Participating Entity to develop and deliver a training format that provides the best solution for each training location. Sentinel's standard training minimally includes the following items: installation and de-installation of equipment; maintenance and cleaning of equipment; use of web-based information system including procedures for enrollment and curfew changes as well as the generation and interpretation of reports; troubleshooting monitoring problems; accessing our technical support and monitoring center; and any additional training as needed to remain current on monitoring equipment and web-based information system.

Sentinel's implementation team will train all agency personnel assigned to the program prior to deployment and as needed for changes to the system, equipment, web-based information system, or personnel, for the duration of the program as directed by the contract. Our standard training protocol includes demonstration, discussion, and hands-on sessions on the following topics:

- + All RF, GPS, Alcohol Monitoring equipment, and client app solutions (use, installation, removal, and troubleshooting)
- + Enrollment (enrollment, deactivation, and the setting of all monitoring parameters including curfew schedules and GPS zones)
- + Tracking and monitoring of participants
- + Alarm processes and resolution procedures (agency-specific protocols)
- + Notification processes and reports (agency-specific protocols)
- + Monitoring System (complete instruction on the use of the web-based information system including, but not limited to, participant enrollment, modifications, reports, schedules, advanced automated analytics, location review, and deactivations)
- + Interpretation of Monitoring Reports (review, define and interpret daily monitoring activity, and Glossary of Terms/definitions)
- + Mobile Application (complete instruction on the use of the Mobile App including, but not limited to, participant information modifications, schedules, location review, device command initiation, field contacts, equipment inventory, and reports/activity review)
- + Accessing Technical Support and Help Desk Services (contact information and access to training support materials)

- The Contractor must provide materials and brochures on the use of the equipment and system.

SENTINEL RESPONSE

Sentinel will provide all user guides, user manuals, brochures, PowerPoint presentations, reference guides, and training videos on the use of the equipment and system for each Participating Entity. Additionally, Sentinel will provide instruction and hand-out material for agency staff to instruct program participants on the use, care, and charging of the equipment.



- The Contractor must provide on-going and supplemental training offerings either on-site or via web based programs on an as needed basis, or based on any significant changes to the Contractor provided equipment and/or technology.

SENTINEL RESPONSE

In addition to the initial training and set up process with a representative on location, the Sentinel Training Department offers either on-site or via webinar training sessions for customers and staff at a minimum of once (1) per year after the initial start-up training offerings, on an as-needed basis, or based on any significant changes to equipment and/or technology. This training is offered for all technologies and services including those proposed herein. It is important to note that Sentinel's webinar training sessions involve interactive voice plus visual contact with a live Sentinel expert trainer, therefore trainees can ask questions and engage in discussion with the trainer as part of any webinar.

Training and webinars are offered at no additional cost to the Participating Entity based on internal training calendars, individual training needs, and scheduled on demand. Webinars are conducted based on contract specifications and/or training needs and can include training on equipment, services, software, web-based system changes, and/or updates. Training is offered for the life of the program as outlined in the Master Agreement. At any time, a Participating Entity can contact our Help Desk for additional support to ensure they are maximizing the technology solution to its fullest potential.

Remaining Category 1: GPS Questions

2. Describe the hardware you propose to meet the requirements of the SOW, including battery life.

SENTINEL RESPONSE

OM500™ Global Positioning Satellite Tracking System

Sentinel is proposing our latest, the most advanced member of the OM Series one-piece GPS device family, that is light weight, discreet, and contoured to fit comfortably on the participants ankle. The OM500™ GPS tracking unit is both the transmitter and receiver of information in one robust feature and function rich unit. The OM500 is equipped with onboard processing capabilities and communicates with the host system via the Verizon or the AT&T LTE networks. This multi-carrier functionality provides a benefit to the Participating Agency because, based on any geographic limitations of cellular/communication coverage in remote areas, authorized staff can use either of the preferred carriers for that region. Prior to program transition, Sentinel will work closely with agency staff to determine which communication carrier works best in that region, thereby ensuring optimal service provision.



The OM500 allows customized tracking and reporting intervals to be assigned at the client level and can store more than ten (10) days of tracking information in the onboard memory, regardless of the mode of operation, should the unit be unable to communicate with the web-based system. The OM500 is also able to store GPS zones on board the device to provide immediate notifications on zone alerts, which is critical in high-risk situations.

OM500 Features: The OM500 is a discrete unit that is easily, securely, and comfortably attached to the ankle of the participant. The OM500 tracking device is a one-piece device that is FCC certified (FCC ID TS5-WP76-OM500) and is small and light weight with the device's dimensions at approximately 3.9 x 2.6 x 1.5 inches and weighing only five (5) ounces, without the strap.



The OM500 is a continuous Global Positioning System (GPS) electronic monitoring solution that is secure, robust, waterproof, submersible, and tamper proof/evident. The unit is ergonomically designed for efficient application, usability, safety, and comfort fit with both standard and large size straps available. For higher-risk participants, the OM500 is available with an optional metal reinforced tamper detecting strap that increases device security by being cut resistant.

For security purposes, the OM500 uses a unique signal to communicate with the monitoring system; other commercially available products do not use the OM500 unit's transmission signal / same coding scheme. The OM500 utilizes encrypted communications to prevent tracing and/or signal duplication. The units are unaffected by atmospheric conditions as well as normal human or environmental conditions, including other devices normally present in a residential setting.

The OM500 has interference detection that will alert the agency should a participant attempt to alter the performance (e.g., mask, jam, or shield) of the OM500 GPS tracking device. If this were to occur, cellular communication and/or the GPS signal could be lost and thus the agency notified of not only of any loss of cellular communication but also of a loss of GPS location information.

—IMPORTANT SENTINEL ADVANTAGES—

Feature Advancements for OM500 GPS: Sentinel has developed the next generation feature advancements for the OM500 GPS device that include:

- + **Increased Connectivity.** The OM500 features state-of-the-art LTE communication connectivity on the Verizon and AT&T wireless networks that provides real-time communication and years of reliable service.
- + **Reduction in charge time by 50%.** The OM500 can be **charged in 30 minutes** if charged daily, acknowledging daily charging is not a requirement as the battery life of the OM500 is capable of **exceeding five (5) days on a single charge**, which is more than twice the industry standard, resulting in fewer low battery alerts that require officer time and action.
- + **Increased battery life by more than 100% over the market average.** The OM500 has an industry-leading **device battery life of 120+ hours (5+ days)** on a full charge in normal operating conditions.
- + **Reduction in Alerts / Increased Compliance.** By providing the longest battery life in the industry coupled with the shortest charge time, the number of program violations is greatly reduced.
- + **Voice Commands designed to improve Communication with Participants.** Using the **OM500 voice commands** allows agencies to send reminders and communicate important information directly over the ankle monitor via automated voice commands as well as detailed text-to-voice audible messaging. This allows authorized staff to send the participant personalized messages in up to nineteen (19) different languages, with all messages tracked and stored in our SentinelDNA monitoring system.
- + **Triple Tamper Detection including: 1) fiber-optic strap design strap tamper; 2) device case tamper; and 3) backplate tamper.** Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and dual pressure sensors within the device, *the OM500 device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tampers with the strap.* The OM500 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate, indicative that the device has been uninstalled/disassembled. Additionally, the unit will send a tamper alert if the unit is broken/cracked or if the unit's backplate is separated from the rest of the device.
- + **Enhanced detection and reporting of device Potential Shielding:** The potential shielding of the OM500 is detected based on various parameters/characteristics of GPS, Cellular and Wi-Fi signals. The system analyzes the RF noise characteristics and levels along with knowledge of signals that are not present to identify if the lack of signal is due to environment or due to shielding of the unit.
- + **Enhanced detection and reporting of device Potential Removal:** In addition to the OM500's three (3) tamper types already developed and implemented, Sentinel has developed an even more robust approach to detect and report possible unidentified removal via the Potential Slippage alert. Within our



internal firmware, Sentinel is maximizing the benefits of the OM500 internal components. By utilizing the accelerometer in combination with cellular signal measurement, "Tilt" measurements, Wi-Fi changes and GPS signal strength, we have developed an even more advanced tamper/removal detection solution to accompany our original leading edge tamper technology.

- + **Optional Reinforced Cut-Resistant Strap:** The OM500 offers an optional reinforced metal strap that reduces unauthorized removal by the participant by reducing the participant's ability to cut the strap.
- + **Pursuit Tracking Mode:** For situations where officers are trying to pursue a GPS participant in real-time, our Pursuit Mode feature allows for the capture of a GPS location every fifteen (15) seconds with transmission of the points every thirty (30) seconds allowing for real-time tracking capability. This feature can be initiated by the agency officers, Sentinel personnel, or by our National Monitoring Center if requested by agency officers while in pursuit. Pursuit Mode tracking can be initiated from any internet accessible device through our web-based SentinelDNA monitoring system as well as from any mobile device through our DNA Mobile App.
- + **Industry Leading Triple Tracking Capability via GPS, Wi-Fi location Points, and Cellular Tracking.** The OM500 also leverages three (3) industry-leading location-based services provided by Google and Skyhook. These hybrid Precision Location systems **locate our devices using Wi-Fi, GPS, and cell signals** ensuring that all devices can be accurately located in virtually every environment. In impaired areas where GPS alone cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. **This allows for a significantly more robust device as it offers multiple tracking options.** Additionally, this enhanced technological advancement and value-add feature eliminates the need for an extra piece of equipment (beacon / home unit) inside the home without any loss of tracking and monitoring.
- + **Advanced Charger Design.** The OM500 charger easily connects to the OM500 **using a magnetic 360° swivel**, allowing the participant to be more comfortable when charging, and the magnetic charging port ensures optimal connectivity and minimal charge time. **The quick disconnect feature eliminates charger or device damage found with other device designs whose chargers are locked into the device and any pressure or tension on the charging cord can break the charging adaptor or the device charging portal.**
- + **Reduction in Design Size/Weight.** Reduced size and weight with less protrusion and a more comfortable fit.
- + **Smart Device Technology** that allows for GPS-based zones "*on board*" the device and immediate reporting of zone violations, along with firmware advancements that extend the battery life to five plus (5+) days on a single charge;
- + **Alerts:** Device reports alerts including strap tamper, backplate tamper, inclusion, and exclusion zones (with optional buffer zones), curfew breaches and a host of additional reminder alerts including low battery, dead battery, and battery charging events. Alerts can be optionally handled / triaged by our 24/7 Sentinel National Monitoring Center staff.
- + **Direct Device Communication:** Participant communication through a multi-colored LED, vibration, beeping, and customized text-to-speech audio messaging
- + **90+ Decibel Siren:** Officers can initiate a 90+ decibel siren directly from the web-based system at anytime to assist with device recovery or participant apprehension and equipment recovery;
- + **Participant Acknowledgement Sensor:** By touching the Touch Sensor located on the front of the device, the participant can confirm receipt of multi-color LED light messaging, voice messages, vibrations, and beeping;
- + **Voice Messaging:** Automated voice messages are delivered via the OM500 instructing the participant to charge his/her device;

—IMPORTANT SENTINEL ADVANTAGE—

The OM500 is designed to accept advanced participant communications configured and initiated by an agency officer via DNA and the DNA Mobile App; it is delivered directly to the participant via the OM500 GPS unit:



- + **Automated Template Voice Commands that can be managed at the master level or sub-agency level.** Automated commands such as *Charge Your Device as Directed*, *Charging Has Begun*, *Charging Has Stopped*, and *Battery Warning/Battery Alert* are delivered to the participant's device when the device reaches the low battery threshold as well as when the device is placed on or removed from the charger.
- + **Automated / Officer-initiated on-demand communications**, including:
 - o Audible Beep
 - o 90+ Decibel Siren proven to be very helpful to field officers during equipment recovery efforts
 - o Vibration
 - o Multi-color LED light
- + **Custom Text-to-Voice Audible Communications in 19 languages.** In addition to simple audio or tone notifications sent to a participant's device, authorized users can send clear, customized audible messages to the participant's OM500 device in 19 different languages.

When a communication is sent to the device, the DNA monitoring system logs the event action with a date and time stamp indicating when the command was sent. When the participant receives the communication, he/she touches the acknowledgement sensor on the front of the device indicating receipt of the signal. If they fail to touch the sensor, the device will continue to flash, vibrate, and/or beep for sixty (60) seconds.

Once the participant touches the acknowledgement sensor, the light flash, vibration, or beeping will cease, and the DNA web-based system will log that the participant acknowledged the command with a date and time stamp indicating when the acknowledgement sensor was touched. The vibration or audible beep features can also be used as a direct contact mechanism with the participant by informing them at the time of enrollment that the vibration or beep is to be considered directions to contact the officer as soon as possible.

As a safety and continued performance feature, two separate low battery alerts are generated when the device is at approximately 30% and again when it reaches 20% or less battery power. These percentage thresholds can be adjusted if requested by the agency, to reduce the chance of battery depletion-related situations. In addition, based on the OM500 extended battery life, upon reaching these precautionary thresholds, the device still retains sufficient battery capacity to ensure the participant has sufficient time to recharge the device.

The OM500 will also automatically notify the participant of a low battery situation with a voice command instructing the participant to charge the device. When the device is removed from charging, a voice command will notify the participant of the completed charge cycle. Additional assistance can be provided from our National Monitoring Center where our operators can contact the participant 24/7 with a direct call informing them of the need to immediately recharge their device.

Multiple Modes of Operations Configurable Through the Web-Based System. The OM500 is both the transmitter and receiver of information in one unit and is equipped with onboard processing capabilities. Via our secure, Internet-based SentinelDNA monitoring system, any authorized user can configure or change the data transmission rate plan (tracking and reporting intervals) on any individual unit without the need to come in contact with the participant/equipment. The OM500 can be remotely programmed to a variety of different transmission rate plans, as intensive as tracking at one (1) point per minute and reporting the information every minute as well as a less intense plan that tracks one (1) point per minute and reports the information every ten (10) minutes. Other reporting intervals are also available based on agency preferences. **It is important to note that regardless of the reporting interval setting, alerts such as Tamperers and Exclusion Zone Violations are always reported immediately.** The OM500 is also capable of indefinitely storing more than ten (10) days of tracking information in its robust onboard memory, regardless of the mode of operation, in the unlikely event the unit is unable to communicate with the web-based system. The OM500 is also able to store inclusion and exclusion zones on board the device to provide immediate notifications regarding zone alerts.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Through the DNA monitoring system, our proposed solution provides the flexibility an agency needs for tracking these rate plans or levels of supervision each participant receives to meet individual monitoring needs. This level is defined by the type of monitoring assigned in the participant's equipment profile. The equipment profile not only defines the monitoring intensity but also allows the agency to change the level based on a participant's current monitoring status. It is important to know that at any time the rate plan can be changed to collect points more/less frequently and to report the information at differing intervals. It is also important to note that, **when in an Exclusion Zone or while in Pursuit Mode, the OM500 device increases its acquisition timers and collects location information every fifteen (15) seconds then reports the data to the web-based information system every thirty (30) seconds.** The most common profiles are identified below but may be customized to meet agency requirements as desired.

MONITORING PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point every one (1) minute and transmits data every ten (10) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every five (5) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every one (1) minute and transmits data every thirty (30) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every one (1) minute and transmits data every sixty (60) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Lower risk participants requiring only standard supervision

—IMPORTANT SENTINEL ADVANTAGE—

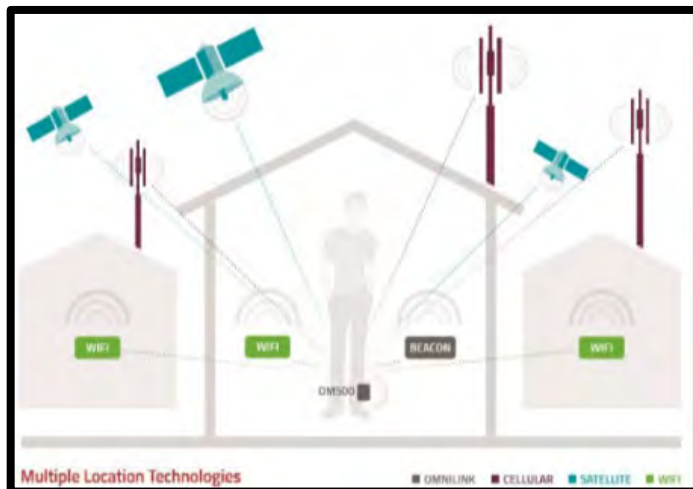
Industry Leading Triple Tracking Capability via GPS, Wi-Fi and Cellular Tracking Location Points. In impaired areas where GPS cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. This allows for a significantly more robust device as it offers multiple tracking options that are included at no additional cost.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Triple Location Tracking Features. GPS, Wi-Fi, and Cellular Tracking. The OM500 is equipped with three (3) location technologies to ensure that program participants are continually tracked, even in the absence of satellite signals. **The OM500 uses GPS, Cellular, and Wi-Fi technologies to track program participants' locations.** This triple-tracking technology provides for consistent and reliable indoor tracking in addition to traditional outdoor-only GPS tracking. Also, when a program participant enters an Impaired Location where GPS cannot be received, the OM500 will automatically switch to cellular tracking and Wi-Fi technologies to continue tracking the participant. Wi-Fi location points are generated using precision location services from Skyhook and the OM500 device will switch to Wi-Fi points when the device is unable to obtain GPS points.



The OM500 collects GPS location data once per minute and leverages both cellular and satellite signals for always-on, high-precision tracking. The OM500's unique design combines these multiple layers of location technologies whereby the device does not have to connect to the Wi-Fi signal, and the signal only needs to be visible to the device. In conditions where GPS and Wi-Fi are not available, the device will automatically switch to cellular tracking location points generated when the device can see one or more cell towers and the location of the point is calculated based on the strength of each visible tower with respect to the location of the device. Such technology allows for reliable location information to be processed virtually anywhere and automatically compensates for insufficient satellite availability in GPS-impaired environments. The combination of these advanced location technologies allows for the quickest acquisition time without being required to go outside to acquire a GPS signal when enrolling and installing a device.

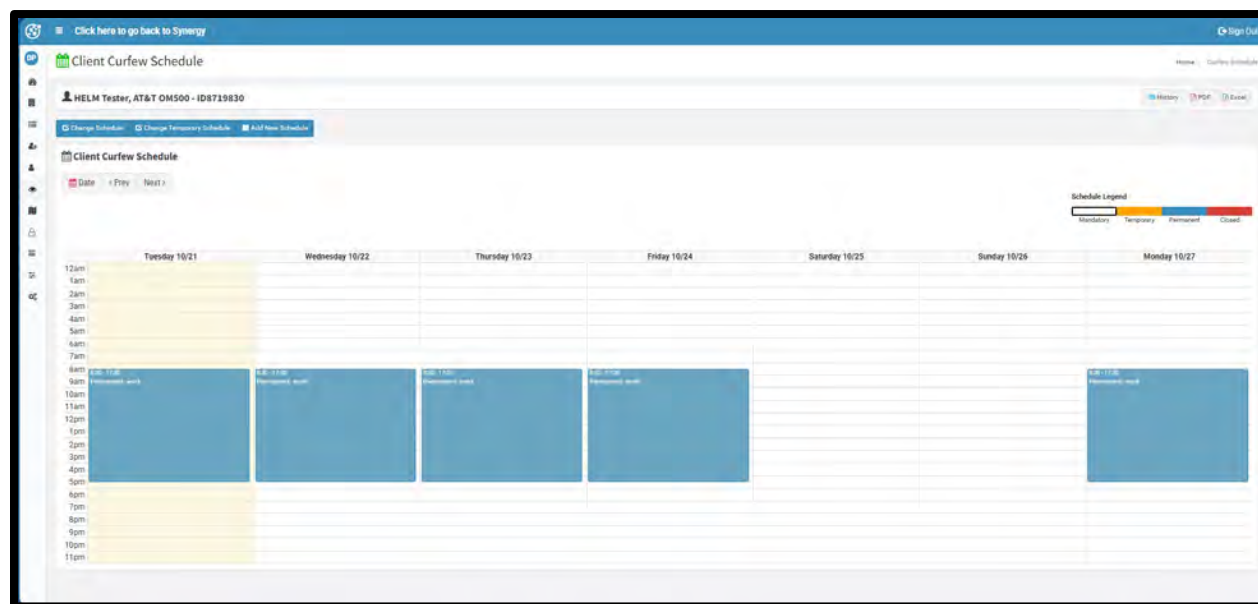
Zones and Curfew Schedules: Through our SentinelDNA web-based system, agency personnel will have the ability to create curfew schedules, zones, and zone schedules for each participant. As shown in the screen images below, DNA provides the capability to create permanent and temporary schedules for each program participant. Authorized users can also copy and paste a schedule from one day to the next thus providing options for the type of schedule and minimizing the time required to create the schedule.

Request for Proposals for ELECTRONIC MONITORING

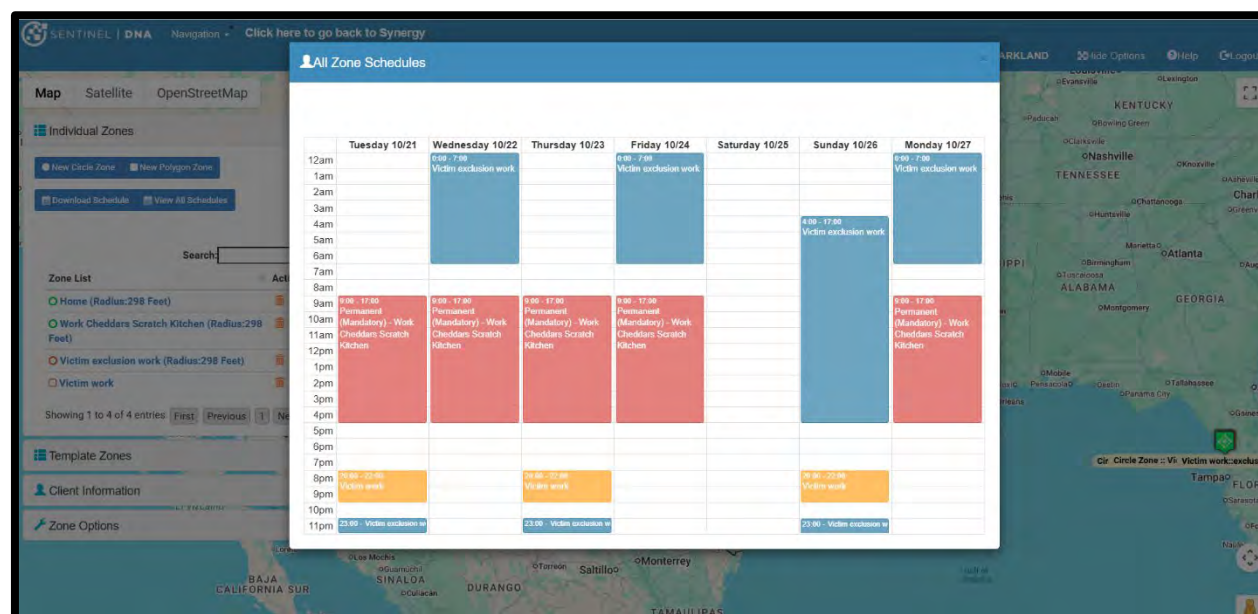
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT CURFEW SCHEDULE SCREEN IMAGE



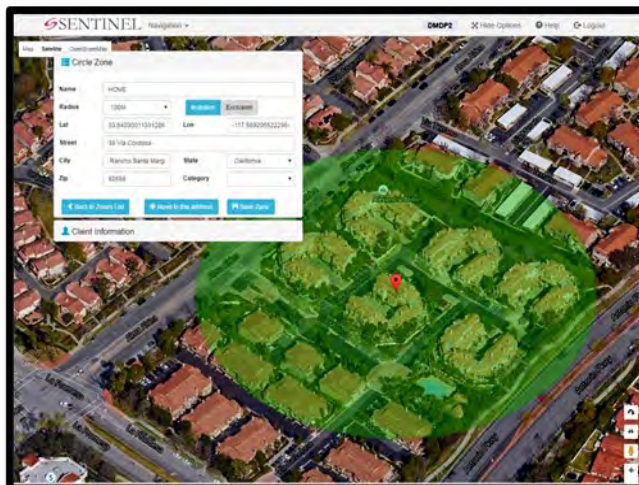
DNA CLIENT ZONE SCHEDULE SCREEN IMAGE



In addition to the ability to create individual schedules for participants, authorized agency officers will also be able to create and configure the authorized locations of participants **via Inclusion and Exclusion zones in the shapes of circles, rectangles, and arbitrarily shaped polygons, as well as be able to have zones within zones.** Sentinel's DNA web-based system will also allow the agency to create / establish advanced warning parameters by including **buffer zones** around exclusion zones to alert individuals of an upcoming potential violation of the zone. DNA also allows agencies to utilize mobile exclusion zones in addition to stationary exclusion zones.

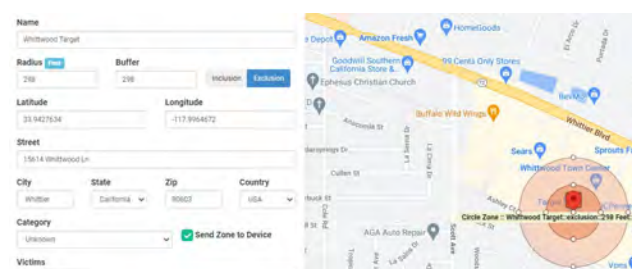
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



GPS Buffer Zones: Buffer zones provide an extra layer of notification around exclusion zone borders and **enhance notifications to allow for a 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. This places 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 buffer and exclusion zone area.

EXAMPLES OF MOBILE EXCLUSION ZONE AND BUFFER ZONE IN DNA



Mobile Exclusion Zones (MEZ): Mobile Exclusion Zones (MEZ) allow agencies to track if a participant on GPS monitoring comes near another specific individual anywhere, they may be in the community. Often used for victim notification applications and in domestic violence cases, the victim has a zone which is created around their smartphone while the perpetrator/participant wears an OM500 GPS tracking device.

Sentinel incorporates the use of the MEZ format through our **Advocate™, Victim Notification and Tracking Application**, which enables the configuration of the Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilizes the victim's smartphone to acquire and report GPS data to our DNA monitoring system. Advanced GPS monitoring technology tracks the location of both the offender and the victim. If the OM500 device comes within an agency specified distance of the victim's smartphone, the victim receives notification on their smartphone of the Mobile Exclusion Zone breach giving her/him necessary information to help initiate her/his safety plan. Additionally, law enforcement may be contacted at the discretion of the Agency.

The Sentinel offender/victim tracking solution gives officers the ability to continuously monitor an offender's proximity to their victims. The locations of the offender and the victim are recorded as historical data giving officers insight into how much time an offender is spending in the vicinity of a victim. The size of the Mobile Exclusion Zone is determined by court order or the agency and may range from hundreds of feet to hundreds of miles. The Mobile Exclusion Zone also incorporates the use of a Buffer Zone in order to create an extra layer of

Request for Proposals for ELECTRONIC MONITORING

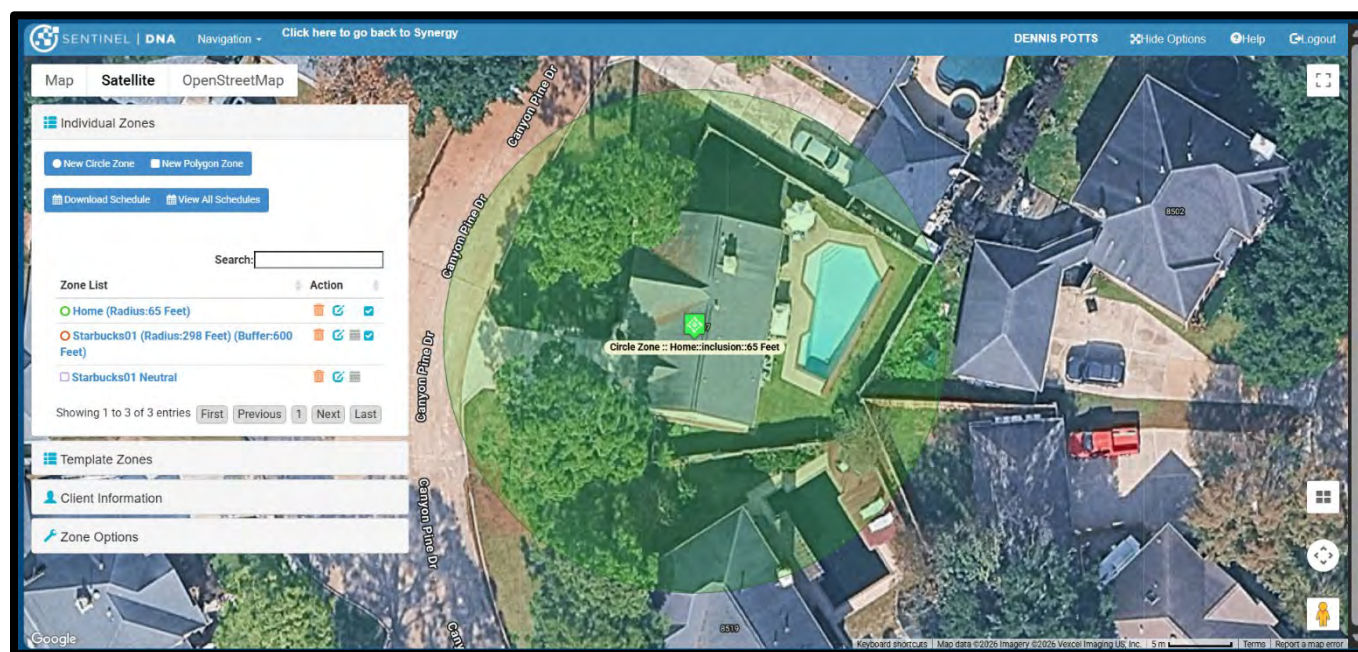
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



notification and enhance the agency's tracking capabilities when utilizing the Advocate Victim Notification and Tracking Application.

OPTIONAL BEACON

In addition, based on its performance capabilities, the OM500 does not require the use of a home unit or beacon to monitor participants 24/7. Through the use of a geographic Home Zone, the system ensures the participant's compliance with curfew or home detention restrictions. A Home Zone is an inclusion zone that ties directly to the participant's primary residence and curfew schedule. Below is an example of a home zone within DNA using the satellite view with the home zone with a radius of 65 feet centered on a residential home.



In order to address the need to provide Beacons in areas of impaired GPS coverage, Sentinel offers our OM500 Beacon that has been designed to be used in conjunction with the OM500 location monitoring and tracking devices. The beacon allows the OM500 tracking devices to obtain location data using Wi-Fi radio frequency signals. Beacons are also an option in dense residential areas and high-rise residential structures to track participant's movements vertically and horizontally.



The OM500 Beacon is designed to be used in conjunction with the OM500 location monitoring and tracking devices. The Beacon is sleek in-home device that provides accurate location data in challenging environments where GPS signals are limited or unavailable. Paired with the OM500, the Beacon uses a secure encrypted Wi-Fi connection to precisely verify presence or absence of the participant at the specific location.

Beacons are an option in dense residential areas and high-rise residential structures where monitoring a participant's movements vertically and horizontally is required. When the OM500 tracking device comes within range of the paired Beacon, the OM500 tracking device establishes encrypted communication with Beacon. The Beacon has multiple alerts to notify the supervising agency if the beacon has been moved or unplugged from the electrical source.

The optional OM500 Beacon is easily installed in a central location in under three (3) minutes by the participant or agency personnel. The unit is powered using a standard two-prong 120-volt AC power cord. The Beacon

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



communicates with the OM500 tracking device via encrypted Wi-Fi signal when the OM500 is in range of the Beacon. The OM500 receives Beacon signals, including the Beacon's status, and communicates those signals and status to the monitoring platform, including the following alerts and events:

- + Beacon Enter and Exit - Device enters or exits the Beacon range.
- + Beacon No Power - Beacon is not receiving power. It is unplugged or there has been some type of power failure.
- + Beacon in Motion - Beacon is continuously moving.
- + Beacon Tampered - Beacon case has been opened.
- + Beacon Low Battery - Beacon is not receiving power and backup battery is low. If battery drops to 30% this alert is generated. The beacon battery has a 20+-hour life when fully charged.

Should the participant/OM500 unit leave the signal radius of the Beacon, the OM500 immediately detects its departure and uses the GPS, Wi-Fi, and cellular technologies to reliably track the locations of the participant.

OPTIONAL OM500 ON-BODY CHARGER

In addition to standard AC charging, the OM500 ankle-worn GPS device can also be charged using an on-body charger (OBC). Sentinel's OBC is **not required and used very infrequently** due to the OM500's 5+ day battery life and quick charge capabilities. The OBC is a small, lightweight device easily attached to the OM500 unit worn by the participant to allow them to charge the device "on the go" without being tethered to a wall outlet affording the participant more freedom of movement.



OM500 GPS DEVICE SHOWN WITH THE ON-BODY CHARGER (OBC)

OPTIONAL OM SERIES CUT-RESISTANT STRAP

Sentinel offers an optional cut-resistant strap that can be used on the OM500 GPS device. Designed for agencies seeking a more robust cut-resistant strap, along with the fiber-optic security of the standard strap, this option incorporates an industry-leading strap design with a thin, heat-treated, hardened, stainless steel insert designed to make cutting the strap extremely difficult. **The cut-resistant strap has a 303 stainless steel half hard insert that is 0.125 inches wide, 0.04 inches thick and 14 inches long, which not only gives it superior corrosion resistance, but higher strength.**



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Similar to the standard strap, the cut resistant strap is made of a thermoplastic polyurethane which is hypoallergenic for comfort to the participant. It is important to note that the OM Series optional cut-resistant strap is variably sized/installed via the same method as the standard OM Series strap thus, significantly more flexible than other manufacturer's tough straps that are bulky, heavy, and NOT variable for sizing, requiring officers to carry numerous interchangeable straps of different sizes to ensure proper fit and compatibility with each participant's unique ankle size.

OPTIONAL SHADOWTRACK® SHADOWWATCH™, WRIST-WATCH GPS DEVICE

We have proposed as an option ShadoWatch™, which is the latest advancement and product offering in the offender electronic monitoring industry and offers agencies a wrist-worn GPS device for monitoring and supervising low risk clients assigned to electronic monitoring. The ShadoWatch is a discreet wrist-worn one-piece GPS tracking device that helps properly monitor low risk program participants compliance. The unit is 2.1 inches by 1.9 inches by 0.8 inches and weighs only 3.7 ounces. Technical specifications features include:



- + GPS/Wi-Fi/LBS Tracking (1- or 5-Minute Intervals)
- + Optional Two-Way Voice Communication
- + Messaging
- + SOS Button
- + Wireless Charger
- + IP-68 Waterproof
- + Tamper Detection (Strap and Proximity)
- + Heart Rate Sensor (Proximity Tamper)
- + Heat Sensor (Proximity Tamper)
- + Motion Sensor

How ShadoWatch Works. The installation process is quite simple and takes only minutes to install. The device should be assigned to the participant in the monitoring database, and the battery should be fully charged prior to installation. To begin the installation process, one side of the strap is locked onto the device housing by attaching it with two (2) screws. The strap is then sized by placing the ShadoWatch and strap around the participant's wrist. One finger width should be between the strap and the participant's skin. Once the proper size is determined, the excess strap is cut off, and the device is installed by inserting the two (2) remaining screws into the open end of the strap and the device housing. Once the device is locked in place on the participant's wrist, security covers are then snapped in place to cover the screws on each side of the device housing. From this point, if the participant tries to attempt to remove the device by cutting it off, a Band Tamper Alarm will generate. Additionally, if they attempt to remove the device by trying to slip it off their wrist, a Proximity Tamper will alert to the unauthorized removal and supervising personnel will be immediately notified.

The device can be set to various tracking intervals based upon the agency's desired preference and location data will be reported to our monitoring platform. Zones can be created to ensure that the participant is in the authorized area(s) at all times. Any compliance deviations can be immediately reported to supervising staff and notifications can be immediately generated by Shadowtrack's automated monitoring center. Notifications can be delivered via an SMS text message, email, and/or via an automated voice call to desired phone number(s). Additionally, field supervising staff can utilize Shadowtrack's Officer Mobile App and/or staff can utilize our desktop web-based monitoring system to monitor the participants in real-time. Supported alarms include:

- + Device Communication Timeout
- + Device Communication Timeout Escalated
- + Failed To Charge
- + Band Tamper
- + Within Exclusion Zone

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Outside Inclusion Zone
- + Lack of Motion
- + Battery Critical
- + Proximity Tamper (No Heart Rate)
- + No Location
- + No Location Escalated

Durability, Battery Life, and Device Charging. ShadoWatch is designed specifically for offender monitoring and carries the IP68 international waterproof, dust, and debris certification. It can withstand submersion in water up to 3 meters for 30 minutes. The ShadoWatch is shock resistant and tamper-proof, with titanium reinforcement within the strap, as well as heart rate and motion sensors to further detect noncompliance.



The ShadoWatch provides ample battery power and staff can be alerted if there are any Low Battery conditions that occur. The unit offers 20+ hours of battery life while providing 1-minute location intervals and 70+ hours of battery life while providing 5-minute location intervals. Though the battery requires a daily charging period of 90 – 120 minutes, the ShadoWatch is equipped with a wireless charger that simply snaps onto the watch allowing the participant to freely move around while charging. The wireless charging block simply attaches to the ShadoWatch to initiate device charging.



3. Describe your software system (web-based applications, smart phone applications). Describe unique design features that ensure accuracy and/or speed of reporting. [Include a description on Priority Communication or similar features.](#) [Edited per Amendment # 3, Offeror Response Worksheet_Revised 2.6.26~2]

SENTINEL RESPONSE

SENTINEL WEB-BASED SOFTWARE SYSTEM

SentinelDNA™ (DNA) is a secure web-based information system that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year. No software components, applications, or client requirements need to be installed by the agency. The SentinelDNA Monitoring System is designed to simplify access and usage across modern browsers on both workstation and laptop computers (Windows, Mac OS X, Linux) and mobile devices (iOS, Android). Additionally, users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves the overall management of program information providing direct access to monitoring data for all authorized agency program personnel.

Designed in-house by Sentinel engineers, DNA can be customized to include all required reports, notification procedures and optional escalation alert sequencing. Moreover, this powerful and easy to use platform will provide the agency with customizable features and benefits not available from other monitoring solutions. DNA makes it easy for officers to access real time information about individual participants or their whole caseload from a secure environment (username and password are required for login). Designed with the needs of end-users in mind, DNA uses a straightforward, intuitive user interface that allows users to efficiently complete all monitoring tasks including:

- + Enroll a participant
- + Create/edit schedules
- + View, create notes
- + Clear events and alerts
- + Locate participants
- + Perform data management administration
- + Create and edit zones (inclusion and exclusion)
- + Adjust tracking rate plans
- + Review device battery status and charging events
- + Create and print reports

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Send custom messages to participant(s)
- + Store and view demographic information
- + Alert processing and advanced triage notification
- + Perform analytics including Point Pattern Analysis and Event Detection
- + Verify and document even contact with participants while in the field
- + Inventory Management including Equipment Recovery Dashboard
- + Store and view photos and documents
- + Victim assignment and notification
- + Perform audits

Sentinel's monitoring system records all data with a historical transaction record and is stored/archived for retrieval/backup in a database when requested by agency personnel. SentinelDNA Monitoring Application maintains a permanent searchable and reportable record in the form of a: 1) Client Audit Report; and 2) User Audit Report. In addition, all monitoring events and notifications are logged with date and time stamp and are also available for auditable review.

Sentinel's DNA platform offers advanced features and capabilities unavailable in other monitoring and tracking platforms:

- + **Sentinel Designed and Owned:** Engineered, maintained, and monitored exclusively by Sentinel allowing for system personalization as required by the Participating Entity.
- + **Login Authentication:** The system is completely secure and uses state-of-the-art security measures. Sentinel has employed the use of Single Sign-On (SSO) and Multifactor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.
- + **Client Dashboard** provides all participant data on one easy-to-read screen. Using straightforward alert icons, the DNA Client Dashboard provides an easy to read at-a-glance interface that allows users to quickly see the status of each participant. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, location information (via mapping), current equipment status, current battery status, as well as zones and curfew schedules.
- + **Point Pattern Analysis (PPA)** provides near real time and historic location automated analytics regarding known locations and variances/variations in movement patterns. PPA is an automated analytics capability that enables users to quickly and easily identify changes in participant location/movement patterns that may be indicative of changes in behavior/compliance. PPA provides authorized users with a more in-depth review of a participant's tracking data.
- + **Sentinel DNA Event Detection (Crime Scene Correlation)** assists with crime/event analysis. Sentinel's Event Detection feature within DNA has a mapping component that correlates crime and/or incident report data collected from local law enforcement agency stakeholders and associates the data with the tracking data of participants. **Our Event Detection mapping feature will identify participants who were in a specified vicinity of an incident address during a specific date/time range.**
- + Advanced **automated screen resizing** enables DNA to be accessed by desktops, laptops, tablets and by most leading smartphone browsers without the need to download custom applications.
- + **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 system allows DNA to provide a participant's current location and location history **via Google's map view, satellite/aerial view, bird's eye view, and street view.**
- + **Near Real Time Scheduling and Mapping** allows for immediate location identification. DNA allows users to view and modify all participant curfew schedules and zone schedules as well as view and print monitoring activity reports for all participants. **DNA has the capability to create permanent and temporary schedules and to copy and paste a schedule from one day to the next.** All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.
- + Advanced and extensive **Report Library**, which can be increased at any time at no additional cost. The **Report Library** provides access to all standard system-generated reports that are pre-formatted and



available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Each data field within the entire information system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system.

- + **Advanced Inventory Control Module** enabling officers/installers 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 equipment orders online via DNA.
- + **Client Field Contact Module** allows agencies to verify and document every contact with participants while in the field utilizing a mobile device with a camera (e.g., smartphone, tablet). While out in the field or in the office, the officer will scan / photograph the barcode on the GPS device which in turn **captures, verifies, and stores the metadata from the mobile device and records in the participant's DNA activity the officer, participant, contact date/time and location, and also stores the photo as visual evidence** that the participant was wearing the device at the time.
- + **DNA Mobile Application** provides officers with mobile access to review participant monitoring data via a smartphone or tablet. Sentinel has developed our DNA Mobile Application for officers to **perform field services and data management work** such as data/schedule changes, equipment changes, de-installations, tracking review, current location requests, etc. from any smartphone or tablet.
- + **Mobile Exclusion Zone Tracking:** Allows agencies to track if a participant on GPS comes near another specific device anywhere they may be throughout the community. Taking tracking beyond just stationary zones, the optional Mobile Exclusion Zone (MEZ) program simultaneously tracks the activity of two (2) GPS devices (or a GPS device and a victim smartphone) to determine their proximity from one another throughout the community.
- + Optional **Sentinel DNA Case Management Module** that is enabled within our existing DNA monitoring application that handles offender caseloads as well as all the data and interactions that comprise an offender population, including the accurate and consistent posting of client payments.
- + Sentinel has a proven **DNA Application Programming Interface (API)** and is prepared to coordinate with the Participating Entity's Information Technology (IT) to implement an interface between the Participating Entity's systems and Sentinel's DNA application whereby common participant data elements and monitoring data may be automatically pushed/pulled between the two (2) systems, thereby increasing officer efficiency by mitigating the need for duplicate keyed entry into both systems.
- + Optional **Advocate™ Victim Notification Application** is compatible with Apple OS, Android OS, and/or Windows-based devices and specifically designed to provide a more efficient and convenient alternative for domestic violence cases. As an alternative to victims carrying a secondary GPS device, Sentinel has developed our **Advocate™, Victim Notification and Tracking Application**, that will enable configuration of a Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilize the victim's smartphone to acquire and report GPS data to our DNA monitoring system that will compare the victim's location to the offender's location. In the event the participant attempts to remove the GPS tracking device or violate any restrictive zone, the victim will receive the notification on her/his personal cellular device. It also allows tracking of the participant and his/her location compared to the victim to reduce the chance of an encounter while in the community.

Client Dashboard. DNA utilizes an advanced **Client Dashboard** feature that provides authorized agency staff with the flexibility to view all or selected subsets of their entire caseload in near 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 each participant without having to research every record to confirm who is in violation and who is not. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, *location* information (via mapping), *current equipment status*, *current battery status*, as well as *zones* and *schedules*.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT DASHBOARD

Name	OID	Type	Equipment	Compliance	Battery	Profile	Officer
Test Group: Advocate App PT, Carlos	ID8768866	GPS3			47%	Web Only	Dennis Potts
Test Group: Advocate App Vic, Carlos M	ID8768872	VAPP			96%	Web Only	Dennis Potts
Dell, Dee	ID8733643	CM				Web Only	Justin Case
Doe, Jill	ID8718393	VAPP			79%	Web Only	LauraZZZ ZZZDennison
Doe, John	ID8717208	CM				Web Only	LauraZZZ ZZZDennison
HELM Tester, AT&T OM500	ID8719830	GPS3				HELM GPS Testers	Training Department
HELM TESTER, RF BART	ID8748994	RF/BART				Web Only	Marielena Tejeda
HELM Tester, Verizon OM500	ID8693586	GPS3				HELM GPS Testers	Training Department
Jones, David	ID8741640	GPS3			6%	Web Only	LauraZZZ ZZZDennison
Kelso, Jackie (Install)	ID8719098	CM				Web Only	LauraZZZ ZZZDennison
Smurf, Papa	ID8732145	CM				Web Only	Christy Suazo
TCP Test	ID8742997	GPS3				Web Only	LauraZZZ ZZZDennison
TCP Level 3, Christy	ID8758249	GPS3				Christy Tester profile	Vanessa Gonzalez
Wonka, Jenna	ID8735419	CM				Web Only	Training Department

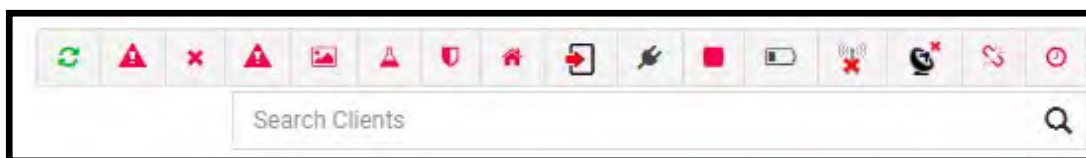
—IMPORTANT SENTINEL ADVANTAGE—

SentinelDNA provides automated program analytics of GPS through our **Point Pattern Analysis (PPA)**. PPA provides near real time and historic location automated analytics regarding known locations and variances in movement patterns. PPA is an automated analytics capability that enables users to quickly and easily identify changes in participant location/movement patterns that may be indicative of changes in behavior/compliance. PPA provides authorized users with a more in-depth review of a participant's tracking data.

Quick Sorting Feature: Authorized users can refine the information displayed on the dashboard by clicking on one of the columns which then sort the participants based on that parameter. **This allows agency staff to quickly view participants by type of monitoring, by alert, or even by battery percentage.** In addition to sorting the information by column, filter icon buttons (shown below) are displayed at the top right of the dashboard, which allow the user to filter participants based upon the selected status/alert criteria.



For example, by selecting the Tamper icon , only those participants with a Tamper alert are displayed on the dashboard. **This allows agency personnel to quickly review alert information each morning and prioritize contact with participants to better manage their caseload.** Below the sort icons, DNA has a local search option (shown below) to make it easy to refine the dashboard display to specific populations or participants with specific first/last names.



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

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT ACTIVITY SCREEN

Client Personal Info

OID	ID8719830
Reference Number	
Name	HELM Tester, AT&T OM500
Home Ph	(800) 589-6003
Work Ph	
Cell Ph	
Address	1220 N Simon Ct/Anaheim, CA-92805
TimeZone	PST

Client Equipment Info

Type	GPS
Transmitter ID	DT000000
IMEI	10000809
GPS Serial No	10000809
GPS Phone	1
Transmission Rate	15 min(s)

Agency

Name	Sentinel Training Department
Officer	Training Department
Cell Phone	714-726-1114
Work Phone	800-555-6566
Email	csuazog@sentineladvantage.com
24/7 Contact	None
Support Staff	None
TimeZone	PST

Client Activity

Event	Event Time	Received Time
Work Failed To Enter Inclusion Zone	10/21/2025 8:30:10 AM	10/21/2025 8:30:09 AM
Work Late To Enter Inclusion Zone	10/21/2025 8:20:24 AM	10/21/2025 8:20:23 AM
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
KMTR Tamper - GPS	10/21/2025 8:02:20 AM	10/21/2025 8:02:47 AM
Backplate Tamper	10/21/2025 8:02:20 AM	10/21/2025 8:02:46 AM

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. **This provides all the important participant information on one screen.**

DNA CLIENT EQUIPMENT STATUS SCREEN

Client Personal Info

OID	ID8719830
Reference Number	
Name	HELM Tester, AT&T OM500
Home Ph	(800) 589-6003
Work Ph	
Cell Ph	
Address	1220 N Simon Ct/Anaheim, CA-92805
TimeZone	PST

Client Equipment Info

Type	GPS
Transmitter ID	DT000000
IMEI	10000809
GPS Serial No	10000809
GPS Phone	1
Transmission Rate	15 min(s)

Agency

Name	Sentinel Training Department
Officer	Training Department
Cell Phone	714-726-1114
Work Phone	800-555-6566
Email	csuazog@sentineladvantage.com
24/7 Contact	None
Support Staff	None
TimeZone	PST

Equipment

Status	Since
HOME	Since 3/14/2025 8:03:46 AM
GPS(Strap) Tamper	10/20/2025 6:05:29 PM Clear
BackPlate Tamper	10/20/2025 6:05:29 PM Clear
Potential Shielding	
Potential Slippage	
MEZ Enter	

As illustrated in the Equipment Status screen image above, the client's current location is shown on the map to the lower left along with the current status of the device including any tampers along with the date and time of occurrence. Officers can quickly view if there is a device issue without wasting time.

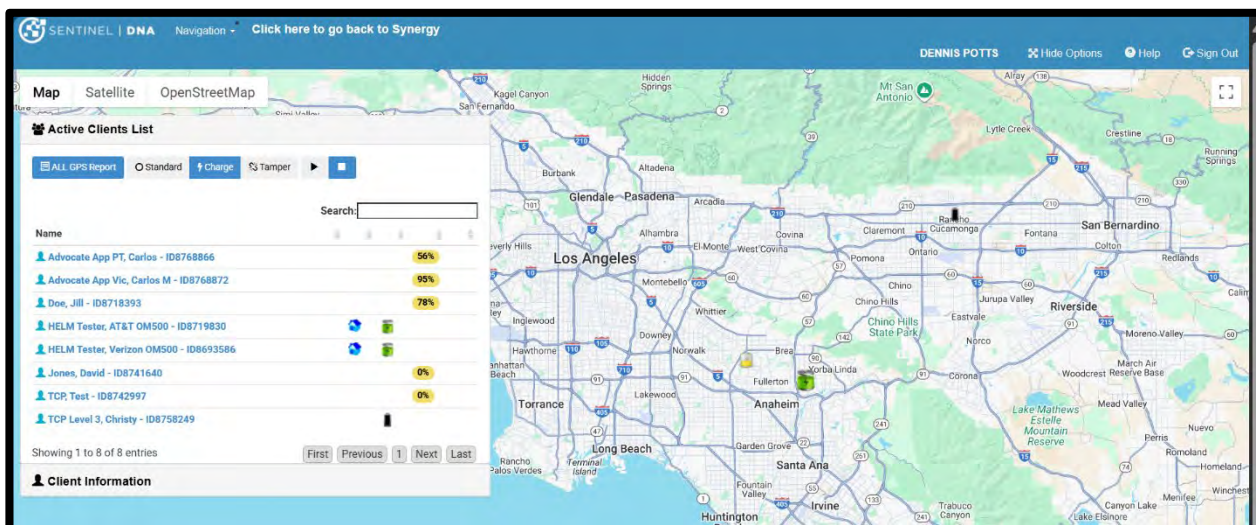
As illustrated below, DNA also gives officers the ability to view the battery status of every device assigned to their entire caseload from a single screen. DNA provides pop-up style notification windows to display caseload details with visual indicators for each participant on a map to the right of the caseload window.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

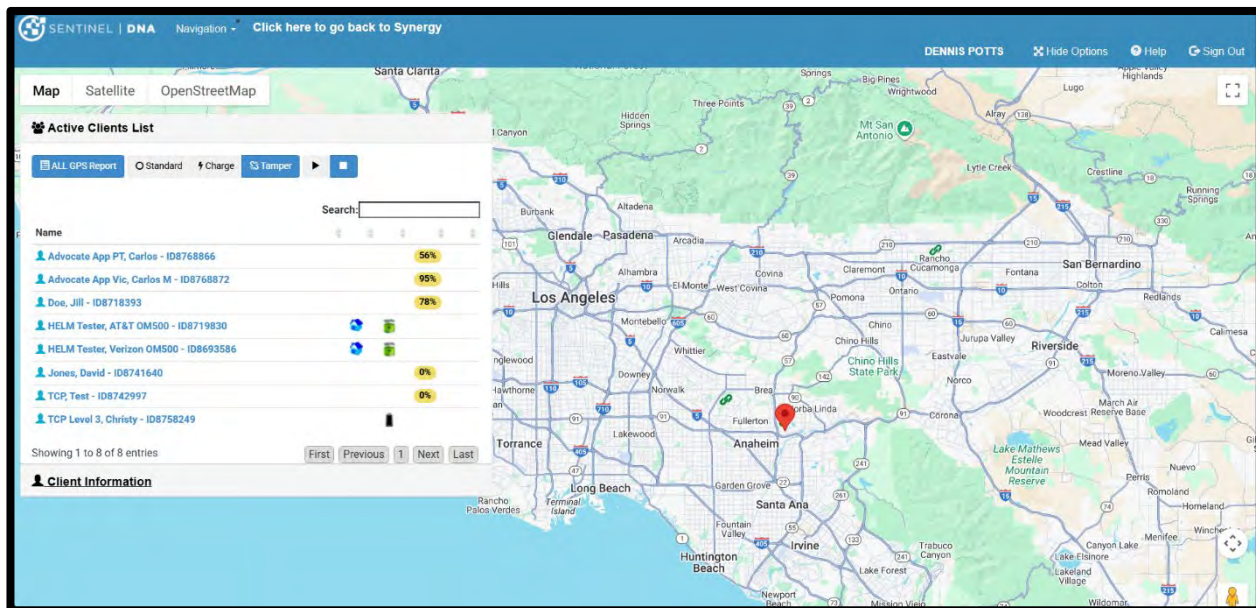


DNA CHARGE / BATTERY STATUS SCREEN



DNA provides the same detail regarding the tamper status of all devices assigned to an officer's caseload. As illustrated below, visual indicators help officers to quickly locate and identify potential issues and/or violations in their caseload. Devices in tamper are indicated with a red icon on the screen below.

DNA TAMPER STATUS SCREEN



Over-the-Air Modification of Device Tracking Rate Plans. Via our secure, Internet-based SentinelDNA monitoring system, any authorized user can configure or change the data transmission rate plan (tracking and reporting intervals) on any individual unit without the need to come in contact with the participant/equipment. The OM500 can be remotely programmed to a variety of different transmission rate plans, as intensive as tracking at one (1) point per minute and reporting the information every minute as well as a less intense plan that tracks one (1) point per minute and reports the information every ten (10) minutes. Other reporting intervals are also available based on agency preferences. **It is important to note that regardless of the reporting interval setting, alerts such as Tamperers and Exclusion Zone Violations are always reported immediately.**

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Through the DNA monitoring system, our proposed solution provides the flexibility an agency needs for tracking these rate plans or levels of supervision each participant receives to meet individual monitoring needs. This level is defined by the type of monitoring assigned in the participant's equipment profile. The equipment profile not only defines the monitoring intensity but also allows the agency to change the level based on a participant's current monitoring status. It is important to know that at any time the rate plan can be changed to collect points more/less frequently and to report the information at differing intervals. It is also important to note that, **when in an Exclusion Zone or while in Pursuit Mode, the OM500 device increases its acquisition timers and collects location information every fifteen (15) seconds then reports the data to the web-based information system every thirty (30) seconds.** The most common profiles are identified below but may be customized to meet agency requirements as desired.

MONITORING PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point every one (1) minute and transmits data every ten (10) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every five (5) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every one (1) minute and transmits data every thirty (30) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Moderate participants requiring intensive supervision
Passive Monitoring	Acquires a GPS point every one (1) minute and transmits data every sixty (60) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Lower risk participants requiring only standard supervision

Advanced Communication Features. Through Sentinel's DNA Monitoring System, the Participating Entity can communicate with the participant via the OM500 one-piece GPS tracking device using **audio voice prompt commands (in multiple languages), a multi-color LED light, an audible 90+ decibel siren, vibration or beeping the device.** These features are activated through the Sentinel DNA monitoring application and can be performed by Sentinel's monitoring center personnel as well as agency personnel. When an audio command, a multi-color LED light, siren, vibration or beep is sent to the device, the DNA monitoring application logs the action with a date and time stamp indicating when the command was sent. When the participant receives the selected communication command, he/she touches the **acknowledgement sensor** on the front of the device indicating receipt of the signal. If they fail to press the sensor, the device will continue to flash, sound the siren, vibrate and/or beep for sixty (60) seconds or in the case of the audio commands, will play the message three (3) times. Once the participant touches the acknowledgement sensor, the communication command will cease, and **the DNA monitoring platform will log that the participant acknowledged the command with a date and time stamp indicating when the sensor was touched.**

Real Time Scheduling, Zones, and Mapping. Authorized users access our DNA Web-Based 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 and zone schedules as well as view and print monitoring activity reports for all

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



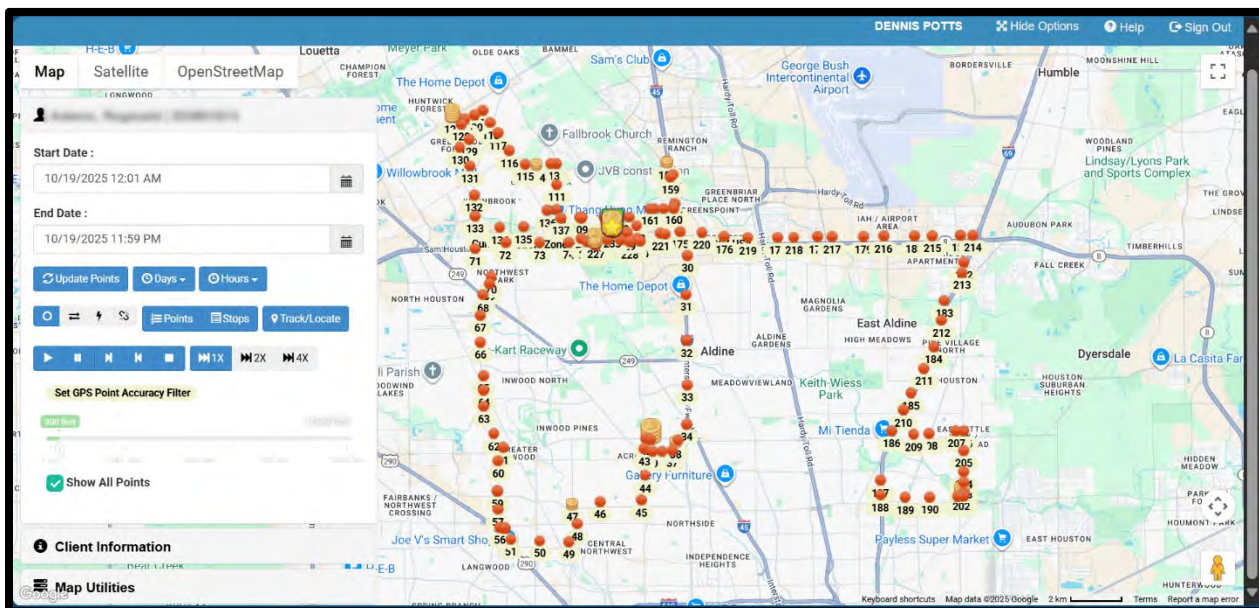
participants. All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.

DNA displays participant location information with a date and time stamp for each location. This chronological display is provided on screen as well as in printed report format.

—IMPORTANT SENTINEL ADVANTAGE—

As an added service feature, DNA allows authorized users to view the actual movements of the program participant, 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 date, time, speed, and estimated precision of each tracking point when the user hovers the mouse over any tracking point. The screen below displays a participant's location history.

DNA VIEW CLIENT LOCATION HISTORY SCREEN



—IMPORTANT SENTINEL ADVANTAGE—

Sentinel's DNA utilizes Google Maps® which provides automatic updates to the system always delivering the latest maps and upgrades. DNA tracks its own points and overlays the points on the most recent Google Maps® available at the time of 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). There are also multiple distinct views including traditional, bird's eye, and street view. These interactive maps contain easily recognizable images at the global level as well as down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking data on the map. With the click of the mouse button, DNA allows authorized users to "drill down" from a high-level view of a participant's overall tracking down to his/her tracking movements at a specific location.

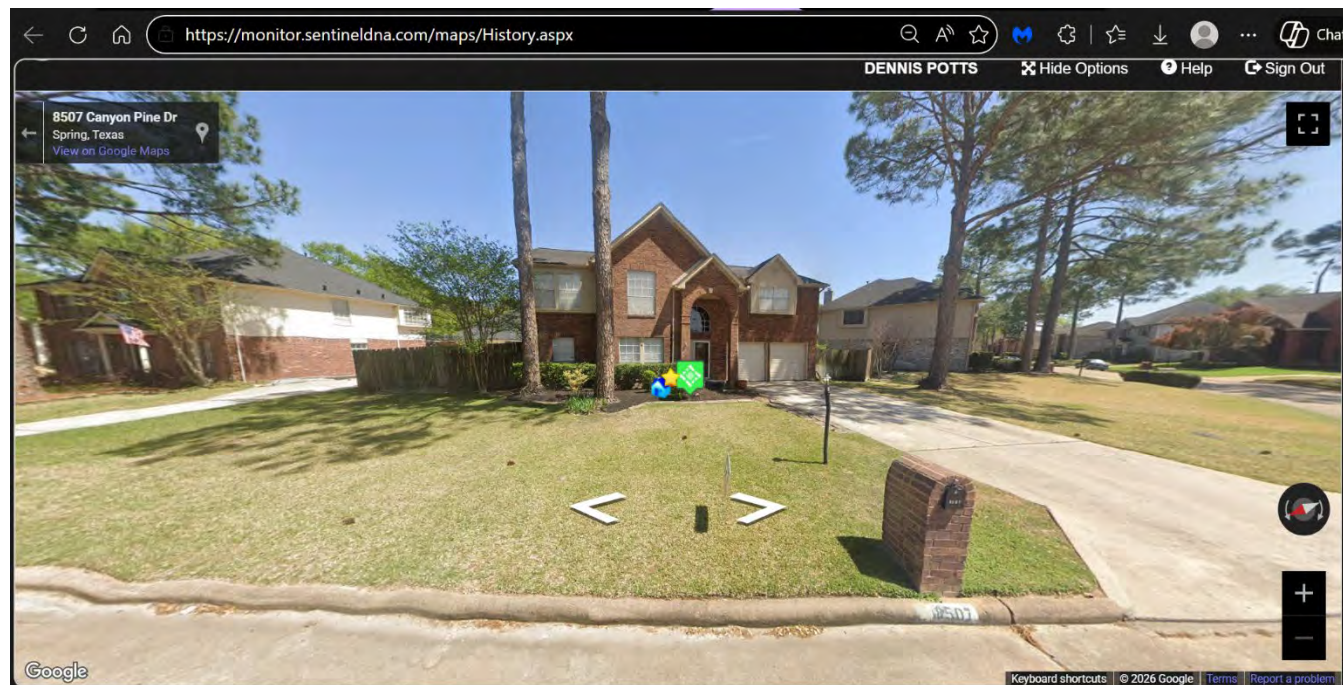
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



—IMPORTANT SENTINEL ADVANTAGE—

DNA STREET VIEW USING GOOGLE® MAPS



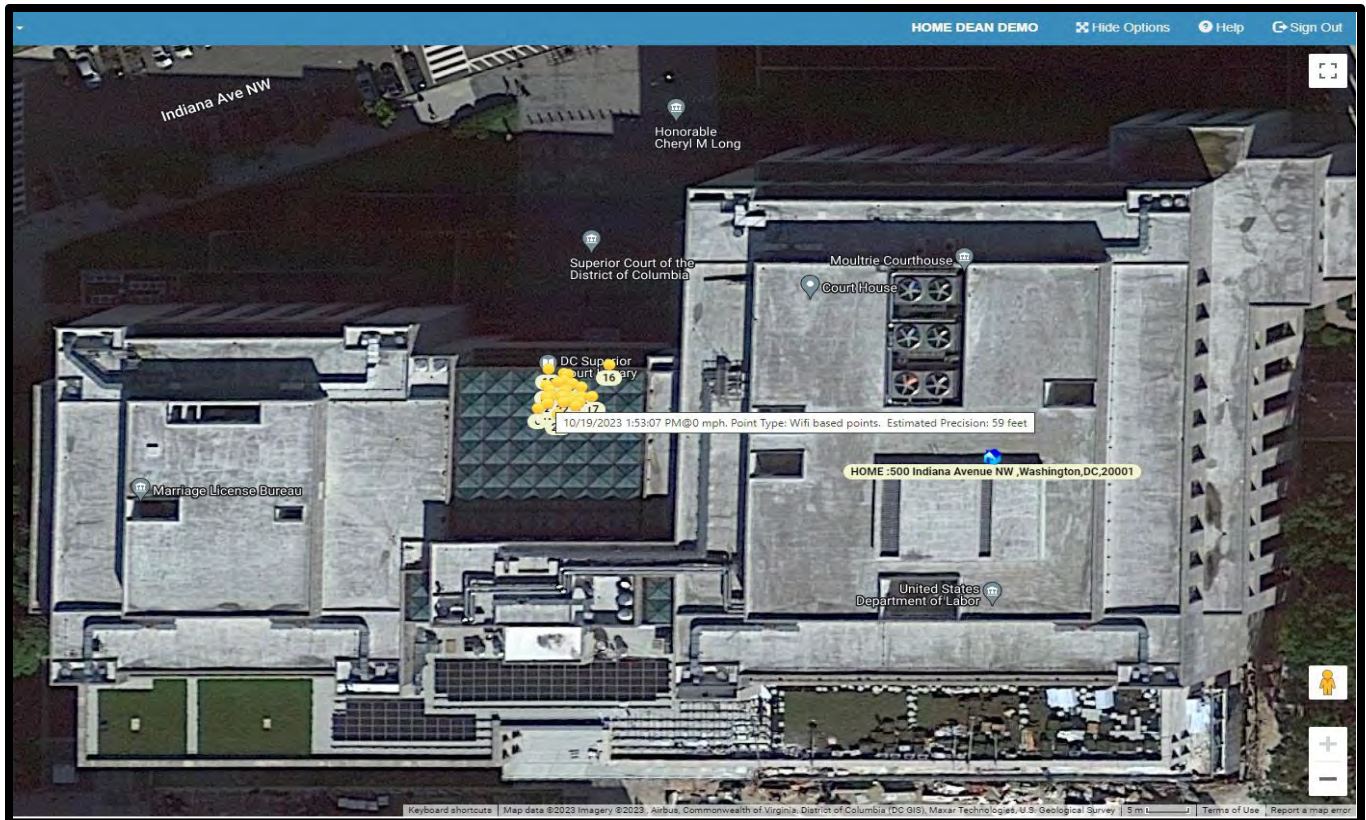
On-Screen Accuracy & Estimated Precision. As an added DNA feature, when a user hovers the mouse pointer over any tracking point an embedded on-screen rollover window appears showing the date, time, speed and estimated precision (onscreen accuracy) of the tracking point. The screen below displays a participant's location history with an on-screen accuracy of "*Estimated Precision: 16 feet*" This advanced feature provides an instant added confidence to officers regarding the relative accuracy of any tracking points of interest. The second screen shows tracking and location monitoring in real time while in an underground subway station.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The following shows the power of the OM500 to continue to track indoors when GPS signals are blocked from large structurally built facilities like the Superior Court in Washington DC. The below shows continuous accurate tracking indoors on the first floor and an accuracy within 59 feet. Without secondary tracking technology, the below accurate tracking would not be possible, as the GPS signals are impaired due to the structure of the building.

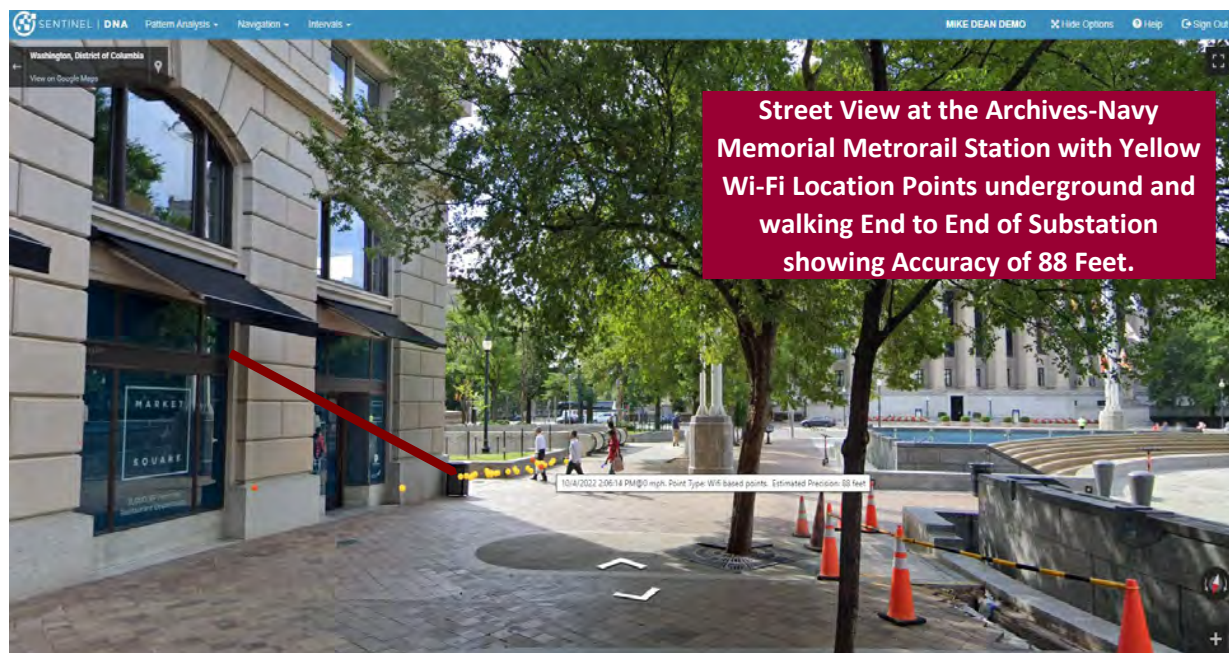


**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



**ABILITY TO TRACK LOCATION IN AN UNDERGROUND SUBWAY SYSTEM IN REAL TIME
AND ACCURATE PROVIDE LOCATION POINTS VIA WI-FI**



Scheduling. During program enrollments, staff enter curfew/zone schedules and/or inclusion and exclusion zone schedules for each program participant in our DNA web-based system. SentinelDNA zone schedules allow supervising entities to select specific periods when a participant is required or is not allowed to be within a geographical location (zone). All zone enter and zone clear events are triggered by points within or outside a

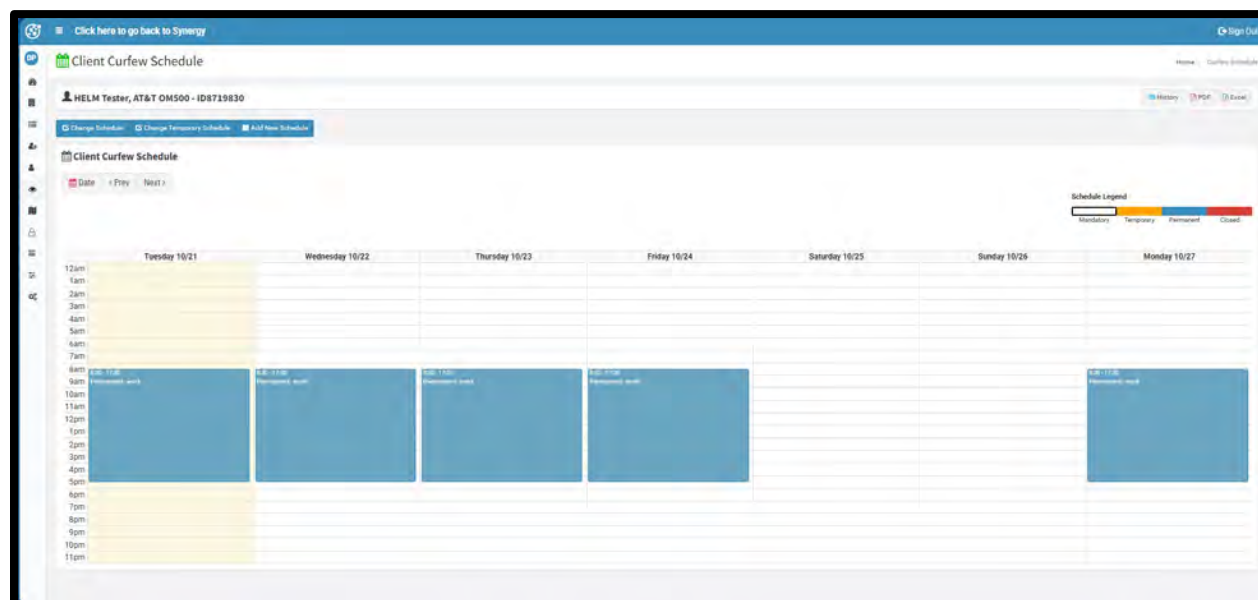
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

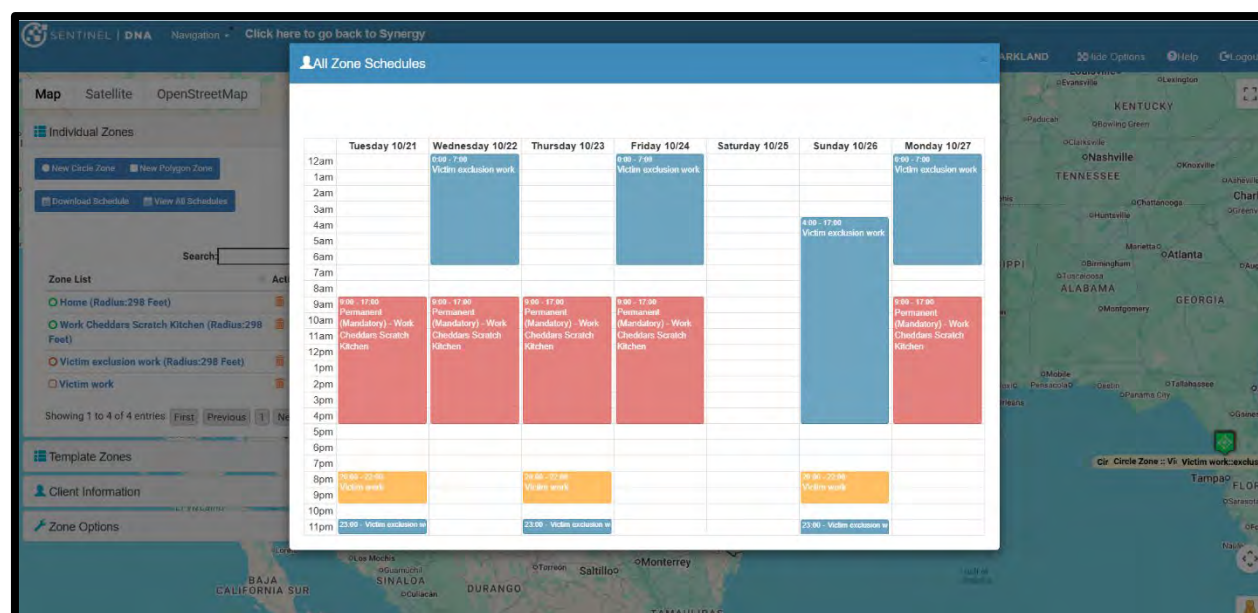


zone. Each exit from, and entry to, the residence or zone (inclusion or exclusion) is reported by the GPS unit, and the DNA web-based system automatically compares the activity's location with the set zones. The OM500 GPS devices, coupled with our SentinelDNA web-based system, provide reliable residential monitoring eliminating the need for home monitoring units or beacons. 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 always ensures the monitoring of each program participant. **DNA also has the capability to create permanent and temporary schedules for both GPS and RF clients and to copy and paste a schedule from one day to the next.**

DNA GPS CLIENT CURFEW SCHEDULE SCREEN IMAGE



DNA GPS CLIENT ZONE SCHEDULE SCREEN IMAGE



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Schedules within DNA define specific time periods when the client is required to be home or is permitted to leave his/her home. If no schedule is assigned to the client, the default setting for each client schedule is “Closed” – meaning the client is not permitted to leave the residence.

The screenshot shows the "Client Curfew Schedule Editor" interface. At the top, it says "DUALTRAK TESTER 1 ANTHONY - ID838820". Below this is a "Copy/Paste" section with buttons for "Copy" and "Paste" for each day of the week. The main area is a calendar grid with days of the week as columns and time slots from 12am to 9pm as rows. A blue bar spans the entire Sunday column from 12am to 9pm, with the text "Client is allowed out all day". A red bar spans the entire Saturday column from 12am to 9pm, with the text "Client is required to be home all day". A red bar spans the entire Tuesday column from 8am to 5pm, with the text "Client is allowed out from 8am to 5pm". At the bottom left, there is a "Change Time Frame" section with radio buttons for 5, 15, 30, and 60 minutes, and a "5" button is selected.

Zones and Mapping. Authorized users will have access to create, edit, and delete exclusion and inclusion zones for participants being tracked via the GPS tracking device. **SentinelDNA allows for a virtually 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 monitor the movement of the individual program participants.

As an added benefit, DNA allows for the creation of template zones that can be used across a specific population of participants. This allows agency personnel to designate certain sites across a region as exclusion zones for an entire population of multiple participants. This eliminates the need to repeatedly re-create the same zones for all the individuals identified in a specific population. This type of **template zone** set-up can be used for sex offenders and other high-risk participant populations establishing zones around schools, playgrounds, or related areas of concern.

—IMPORTANT SENTINEL ADVANTAGE—

DNA allows for the use of **Individual Zones** that create pre-set zone placements for an individual program participant. To simplify the creation and use of zones, DNA places an icon in every zone (individual zone or template zone) to indicate the type of zone shown on a map.

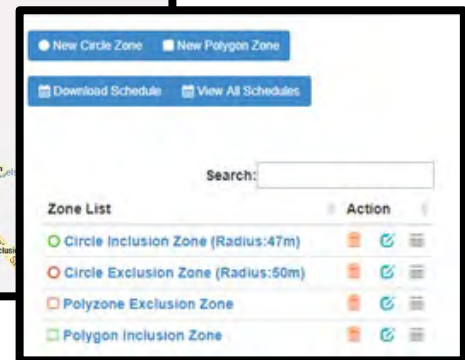
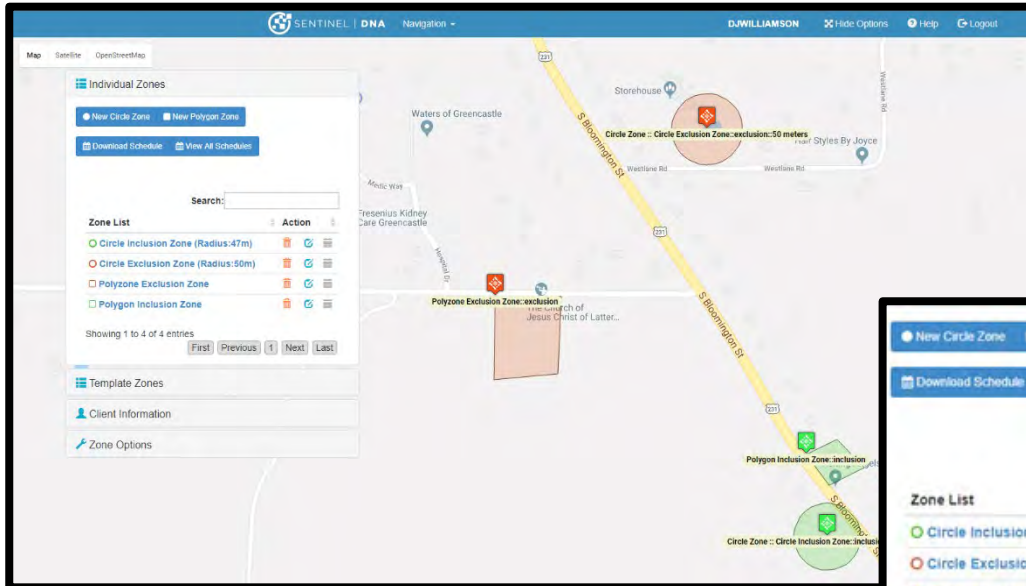
When an agency officer views a participant's tracking data from the mapping screen, the zones, along with the detailed information about each zone, is displayed including the name of the zone, the zone type (inclusion or exclusion), and the zone radius if it is a circle zone. Polygon zones are also available to better track an offender in urban locations and are also displayed within the participant's tracking data from the mapping screen. This allows authorized users to access meaningful location information while reviewing participant zone activity without moving away from the mapping screen.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

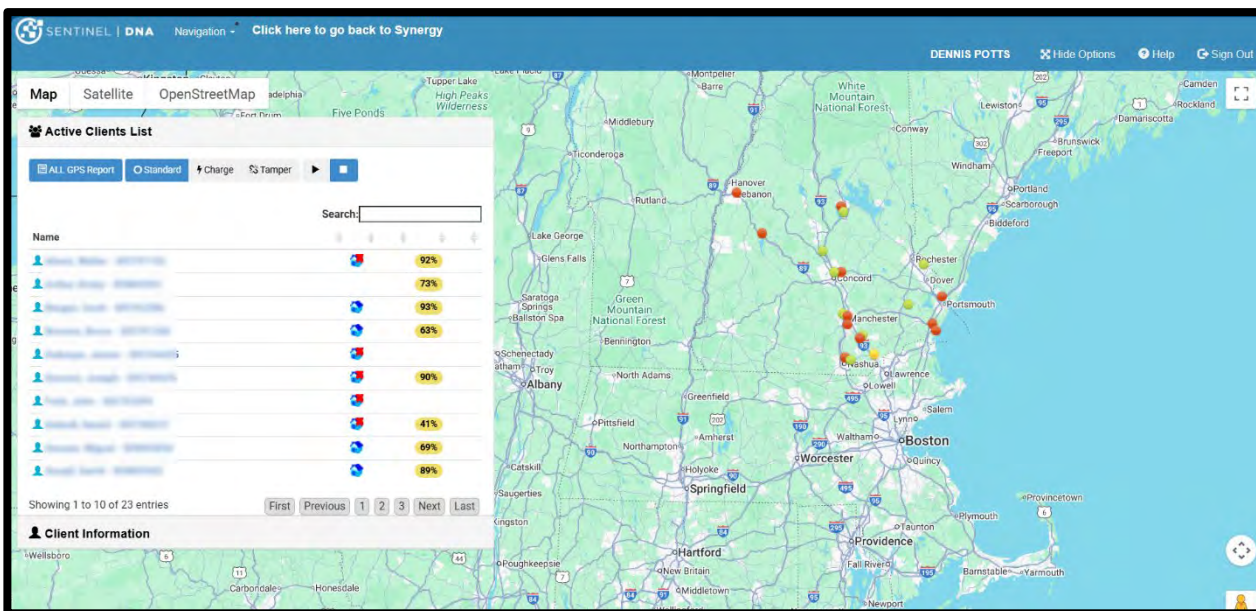


As shown in the images below, DNA visually differentiates zones with color-coding (Inclusion Zones = **GREEN**; Exclusion Zones = **RED**). From the Zones screen, **circle zones are represented in the list by a circle and polygon zones are represented in the list by a square**.



The DNA Mapping System 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 map. For example, in this view shown below, the officer is viewing multiple statuses including the battery status of the device as well as the current tamper status and whether the program participant is at their residence/inside their home inclusion zone or away.

DNA LOCATE ALL CLIENTS SCREEN





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

- + Users may choose to view “Stacked” grouping points on the map for cleaner location display;
- + 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 individual participant “View History” page;
- + Points are centrally displayed during point animation / DVD style playback, and the address and date/time information is displayed below the DVD style playback buttons;
- + Users may choose to view Individual Zones and/or Template Zones on the map when viewing participant location history;
- + Zone icons have been added to help identify zone types. The radius of a circle zone and the name for each zone is displayed beneath the icon on the map;
- + Zones are adjustable to nearly any size;
- + Template and Individual Zones may be viewed from the View Client Zones page; and
- + Participant Location History defaults to the previous 24 hours.

GPS Point Accuracy. The OM500 is a continuous Global Positioning System (GPS) electronic monitoring solution that provides near-real-time reporting of individual locations within a range of plus or minus 30 meters. The OM500 collects GPS location data once per minute and leverages GPS, Cellular, and Wi-Fi technologies to track program participants’ locations for always-on, high-precision tracking. The OM500 GPS tracking device communicates with the 32 U.S. Government global positioning system satellites, including the GPS, Galileo, GLONASS, and BeiDou satellite constellations, and is capable of providing an accurate GPS location point within greater than 30 meters. The unit is equipped with multiple channels to rapidly scan the horizon to determine its location from the visible satellites in orbit.

Sentinel’s OM500 incorporates multiple advanced technologies specifically designed to deliver a high degree of accuracy that automatically measures, calculates, and reflects any accuracy deviation in a number of feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby increasing officer confidence.

- + **Industry Leading Triple Tracking Capability via GPS, Wi-Fi location Points, and Cellular Tracking.** In impaired areas where GPS cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. This allows for a significantly more robust device as it offers multiple communication options.
- + **On-Screen Accuracy Precision reading for every Tracking Point.** The Sentinel DNA web-enabled monitoring and case management software automatically maximizes the accuracy of the multiple location technologies (GPS, Cellular, or Wi-Fi) into one/the same tracking point, generating one of the most accurate points available. Tracking points are differentiated by color according to the type of point, and each point is numbered in order of occurrence. For any tracking point the user hovers their mouse pointer over, Sentinel DNA automatically provides a “Precision” feature that measures, calculates, and reflects any accuracy deviation in a number of feet, visible on screen, enabling officers to identify overall accuracy and any potential drift, thereby significantly increasing officer confidence. Additionally, by hovering over any point on the location history screen, the DNA monitoring application system will display the date and time of the location point, the speed of the point, the type of point that was acquired, and the Estimated Precision or Accuracy of the point.

—IMPORTANT SENTINEL ADVANTAGE—

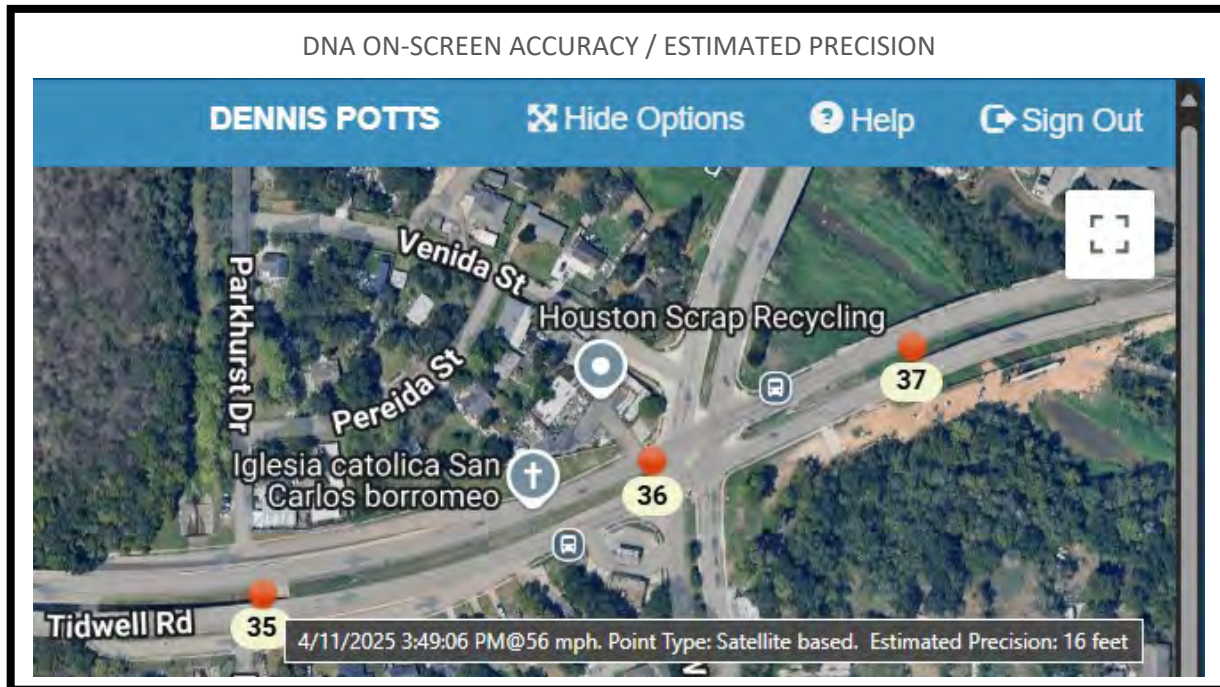
As an added DNA feature, when a user hovers the mouse pointer over any tracking point an embedded on-screen rollover window appears showing the date, time, speed and estimated precision (onscreen accuracy) of the tracking point. The screen below displays a participant’s location history with an on-screen accuracy of

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



"Estimated Precision: 16 feet" This advanced feature provides an instant added confidence to officers regarding the relative accuracy of any tracking points of interest. Also, the second screen shot shows accurate tracking in an underground subway system in Washington, DC with a high rate of accuracy and in real-time.

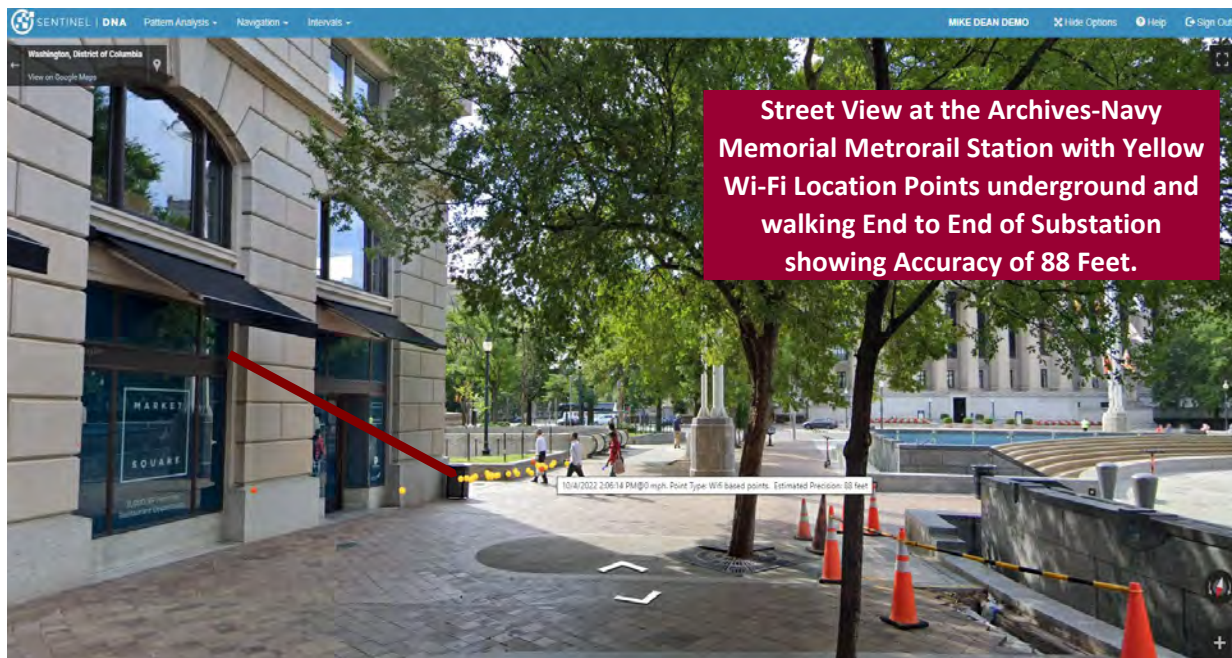
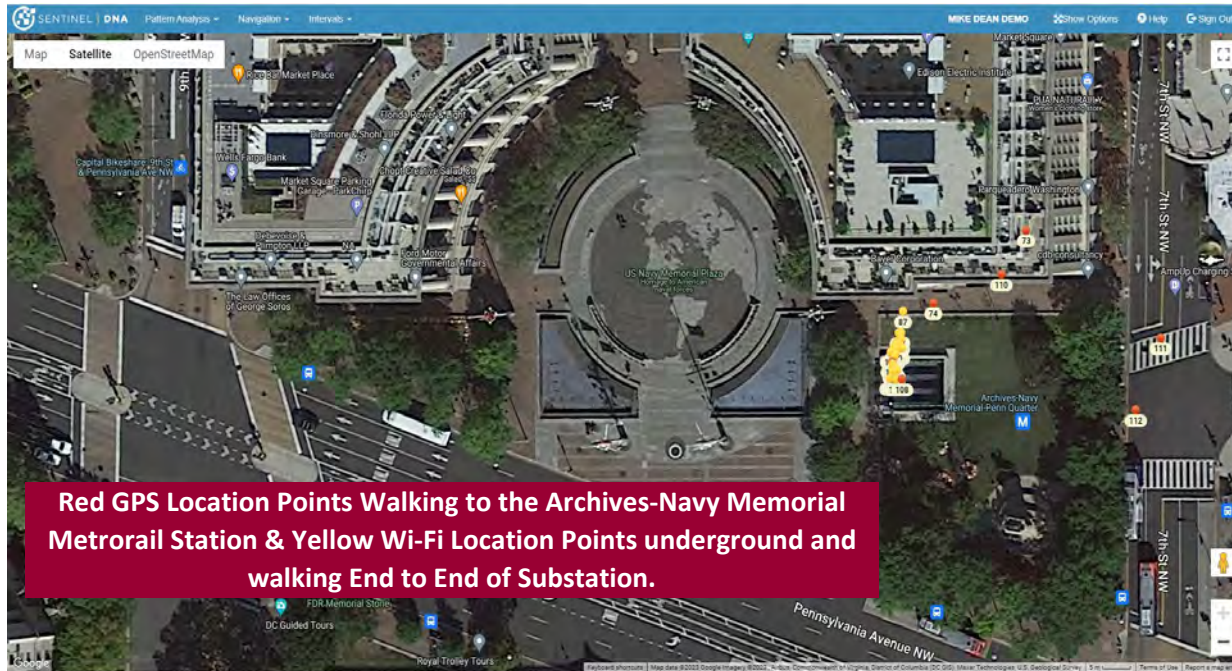


Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



ABILITY TO TRACK LOCATION IN AN UNDERGROUND SUBWAY SYSTEM IN REAL TIME
AND ACCURATE PROVIDE LOCATION POINTS VIA WI-FI



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

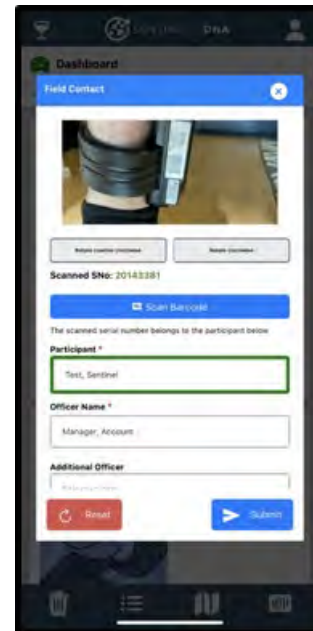


Client Field Contact Module. The Client Field Contact Module within DNA enables agencies to verify and document every contact with a participant while in the field/office utilizing a mobile device with a camera (e.g., smartphone, tablet). While out in the field or in the office, the officer will scan / photograph the image of the barcode on the GPS device which in turn captures, verifies, and stores the metadata from the mobile device. This data includes the date and time stamp of the event (scan), the latitude and longitude location at the time of the contact event, and the photo of the unit itself. **Each upload is also automatically linked with the officer who performed the data entry for historical accuracy.** DNA also allows officers to add data and comments as well as use agency-definable drop-down fields to track specific data points such as if additional staff members were present at the time of the contact.

—IMPORTANT SENTINEL ADVANTAGE—

The Client Field Contact module provides proof of the date, time, and location of each participant contact including the metadata making it capable of standing up in a court of law.

This module is designed to provide accountability for officers and staff. Additionally, this feature authenticates officer/participant contacts because the metadata itself is date and time stamped, in addition to capturing current latitude/longitude, at the time of the scan/entry; if the officer attempted to use old data, the date and time stamp would not match. However, if a barcode is damaged and the officer cannot capture the image, DNA will allow the officer to manually enter the serial number at the time of contact. The information is historically accurate as the supervisor can note the date/time of the entry in the system while the officer was performing the contact and the scan/photograph will also still attach to the record including the metadata associated with it.



Reporting Module and Notification Procedures. SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system.. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

—IMPORTANT SENTINEL ADVANTAGE—

DNA provides additional reporting features for participants who are being tracked with GPS. From the Reports menu and the mapping screen, authorized users can run reports for a single participant or group of people:

- + Alerts showing which actions were taken and whether the notifications were successful
- + Reports showing all events, including alerts
- + Proximity, allowing users to see whether any or all participants were near a specific location at a specific time (Event Detection / Crime Scene Correlation)

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

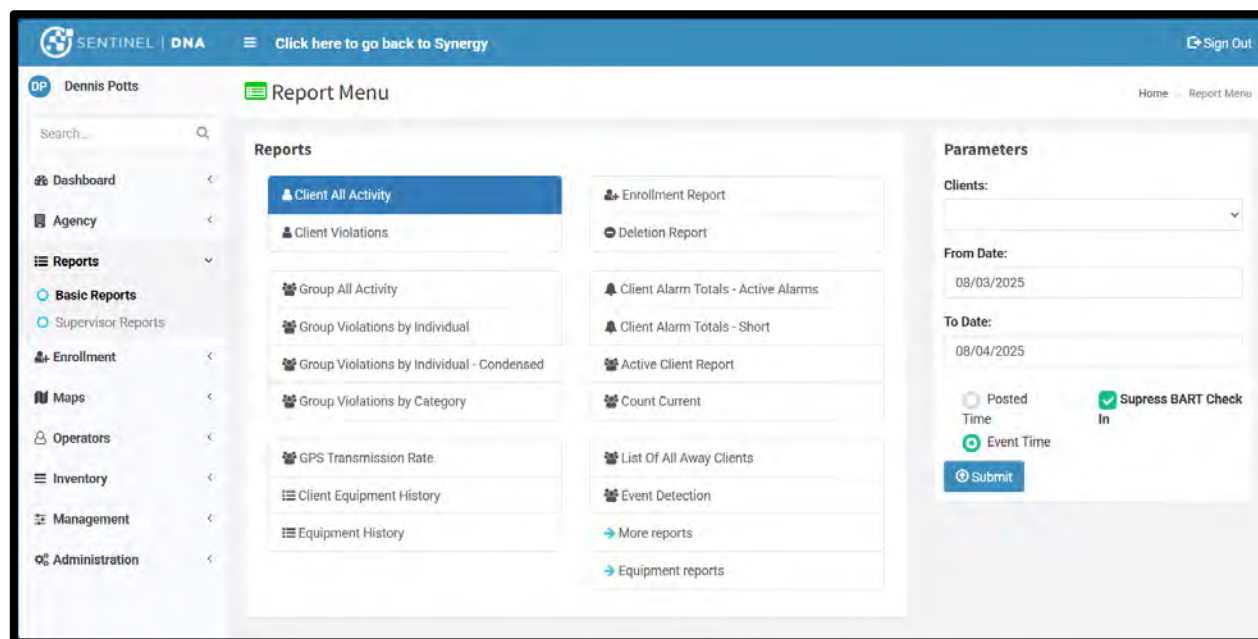


- + Zone activity to show which participants entered and exited zones, such as AA, shopping malls, known drug areas, etc.
- + Stops Report that shows where and when participants stayed in one (1) location over a given time period
- + User Audit Report that shows which users are logging into the monitoring system and for how long

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

DNA REPORT MENU SCREEN



If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

Sentinel's DNA web-based information system is also equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts and violations. Violations can be prioritized to alert immediately or hold for a grace period. The DNA Profile Manager allows for automated notification of alerts as well as optional manual escalation/closed loop communication and sequencing. The Profile Manager also differentiates protocol changes within a single alert by time and day of the week. Please refer to the image below for Sentinel's **Notification Procedure** screen within DNA. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA NOTIFICATION PROCEDURE SCREEN

The screenshot shows a web application interface for "Profile Viewer" within a system called "Synergy". The page title is "Do Not Pass Go Bonding (Version: 1)". It was created on 3/21/2024 at 8:15:26 PM. There is a "Back to Profile Manager" button in the top right. The main content area is titled "Backplate Tamper - GPS11" and has two tabs: "Steps" (selected) and "Clearing Alarms".

The "Steps" tab displays a timeline of events for two days: Sunday and Monday. Each day shows a table of states, actions, state times, and next states.

Day	Time	State	Action	State Time	Next State
Sunday	00:00:00 - 23:59:59	Step 1	Auto Email and McApp	0	Step 2
		Step 2	Delay	10	Step 3
		Step 3	McApp	0	
Monday	00:00:00 - 23:59:59	Step 1	Auto Email and McApp	0	Step 2
		Step 2	Delay	10	Step 3
		Step 3	McApp	0	

Instructions for each day: "Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue." and "If no tamper clear, contact officer on duty at the number provided. Close."

Advanced Automated Analytics. Sentinel's proposed solution includes GPS analytics featuring client stop patterns and shared locations. Sentinel's **DNA platform offers advanced analytic features and capabilities** unavailable in other monitoring as described below.

Point Pattern Analysis (PPA) is an automated analytics capability that enables users to quickly and easily identify changes in participant location/movement patterns that may be indicative of changes in behavior/compliance. To provide an agency with the most opportunities possible to create effective monitoring and in turn positive outcomes for participants, DNA includes Point Pattern Analysis (PPA) capabilities at no additional cost. This proprietary enhancement feature allows users to receive a comprehensive analysis of all their participants' routines.

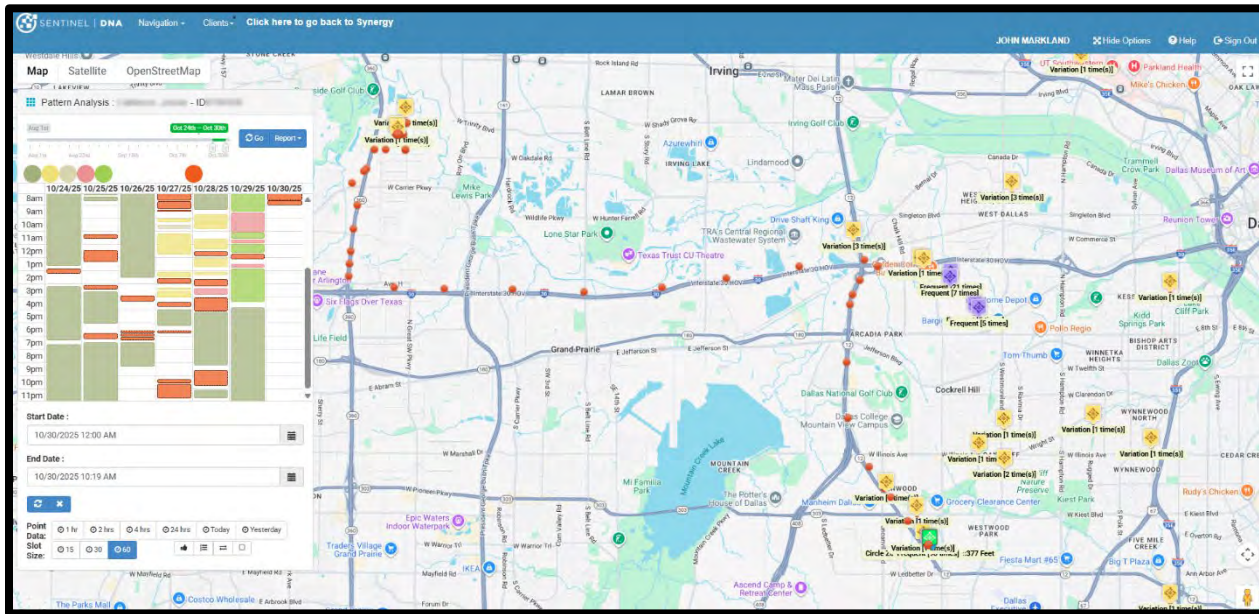
Using our GPS point capture capability, our system can accurately track and display the participant's whereabouts 24/7. Although this is provided as part of the standard GPS tracking service, the advancements associated with PPA provide authorized users with a more in-depth review of a participant's tracking data. It will quickly identify "locations visited" by the participant and identify travel patterns. **PPA displays, in a detailed chart format, the periods of time when a participant was at a certain location.** The system is then 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 participant compared to variations that may be restricted locations.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Point Pattern Analysis examines locations frequented by each individual participant. 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-coding system, while locations that are new for the program participant are color coded in **RED**.



As an example, on the map display depicted above, a user can click on the locations and the position is displayed on a Google Maps 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.

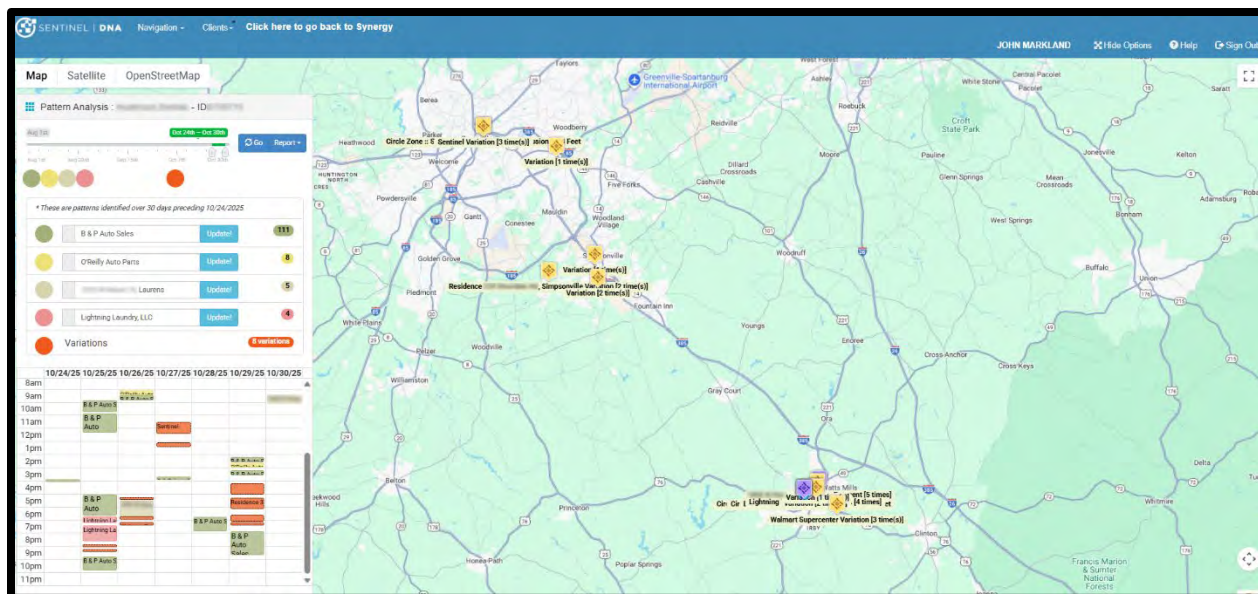
Quick and Detailed Activity History: The system can track on an ongoing basis the data points previously visited by the participant to identify and display any new locations. This allows staff to quickly see the variations in the participant's movements across the community and verify where he/she is stopping throughout the day. This PPA feature is key to assuring that the participant is not straying from his/her required schedule.

For example, if the participant is only allowed to attend work, this system should display only two locations visited, his/her residence and his/her job site. It allows for identification of travel time, which also can be used by the officers or designated personnel to confirm that the participant is not loitering during transit times between these two (2) authorized locations.

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



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



All data collected as a part of the PPA feature can be exported in a report form. **The data will identify known locations based on the labels assigned to those locations as well as identify locations identified as variations using a street map view.** Both known locations as well as variations are displayed within the report with the date and time of each event as shown in the image below.



Request for Proposals for
ELECTRONIC MONITORING

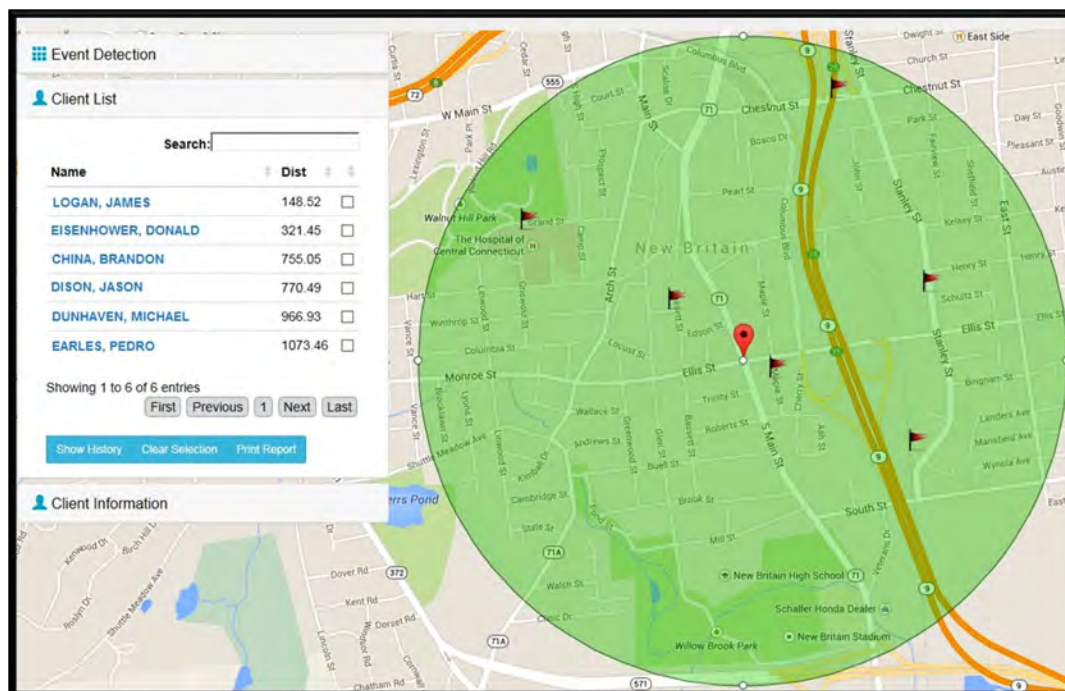
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Sentinel's **DNA Event Detection (Crime Scene Correlation)** feature within DNA has a mapping component that correlates crime and/or incident report data collected from local law enforcement agency stakeholders and associates the data with the tracking data of participants.

Our Event Detection mapping feature will identify participants who were in a specified vicinity of an incident address during a specific date/time range. Event Detection will simultaneously provide information for participants who are in the vicinity at the date/time of occurrence of the crime. Once the data has been entered, and the search has completed, the system will provide a Participant List and place a flag on the map for each participant in the results list and represent the location of the participant that was closest to the search address during the time frame selected.

The search results are displayed under a precise "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 address radius within the time frame selected, thereby creating a list of potential individuals for law enforcement follow up. The system also displays the participant's actual distance from the address of interest, as shown below. Furthermore, all other GPS participants can be eliminated as potential individuals as they were not in the vicinity at the date/time in question.



In addition to our ability to track multiple clients through our Event Detection Module, Sentinel is in the final stages of releasing our Co-location module within SentinelDNA with release scheduled for Q2-2026. **Co-Location is an automated analytics capability that enables users to efficiently identify instances in which multiple GPS participants were present at the same location at the same time, or at the same location at different times. Identified co-location instances will be presented through graphical, map-based, and tabular data views.** These patterns may indicate potential changes in participant behavior or compliance.

This tool will allow officers to analyze the behaviors / daily routines of several clients at one time to determine if the participants are co-locating and quickly identify deviations that may indicate a compliance issue. This tool will also aid officers who are tasked with tracking gang and criminal behaviors as the module will allow officers to view on a map all the participants who are potentially interacting with known criminals as well as the locations of where

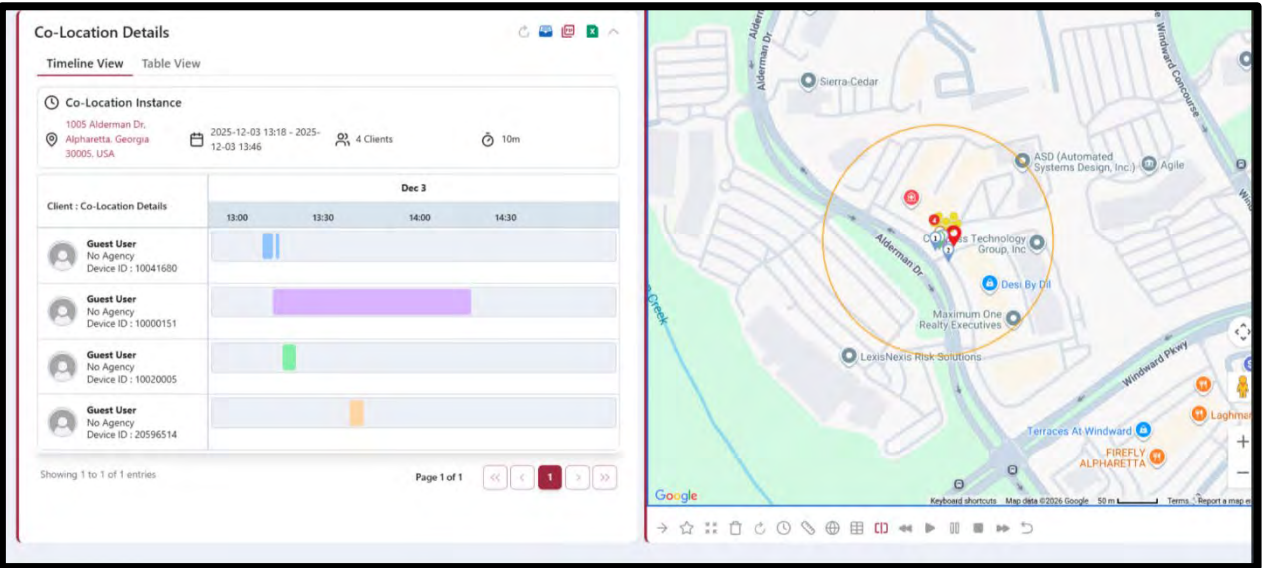
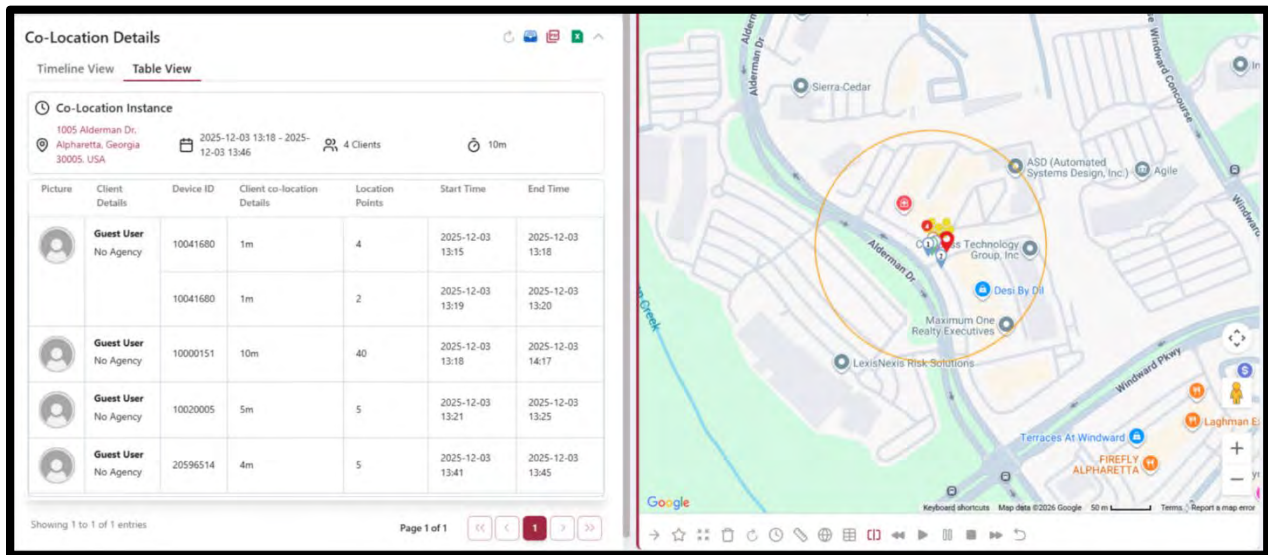
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



the participants choose to meet and/or congregate.

Below is a screen image of the upcoming **Co-Location Module** showing how several groups within the demonstration program have co-located – including the map as well as start / stop times.



While the Co-Location Module is currently in development and will be available to our customers in Q2-2026 Sentinel will provide updates on the progress and development status for the Module and include it within our Analytics offering upon completion.

Inventory Control Module

—IMPORTANT SENTINEL ADVANTAGE—

DNA includes an integrated agency Inventory Dashboard providing textual as well as graphical status of all agency equipment inventory and the online capability for users to view status, manage, order, return, track, and

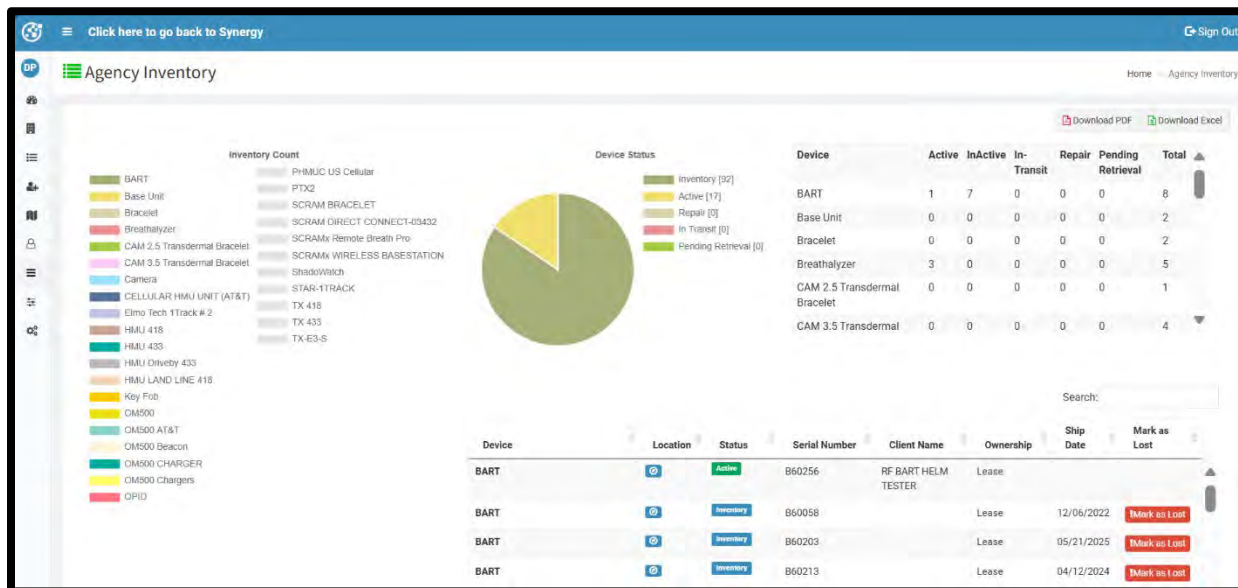
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



transfer equipment. This advanced module will also enable users to request/process/track/manage equipment orders online via DNA. Please refer to the sample DNA agency Inventory Dashboard Screen below.

DNA AGENCY INVENTORY DASHBOARD



Equipment Retrieval Dashboard

Sentinel has created a unique tool within our DNA monitoring platform to assist agencies with their equipment recovery and inventory control efforts. The **Equipment Retrieval Dashboard** has been designed to provide a visual step-by-step inventory retrieval process for both Sentinel's on-site personnel as well as agency staff. **The Equipment Retrieval Dashboard allows agencies to establish more accurate inventory controls and in turn better manage participant equipment recovery thus reducing equipment loss.**

The Equipment Retrieval Dashboard is located in the Inventory section of our DNA platform. The Dashboard displays a complete list of all devices that were not retrieved from participants upon program completion/violation or who have absconded from the program.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Retrieval Dashboard Home Retrieval Dashboard

[Show Archived Retrievals](#) [Profile Manager](#) [Dashboard Settings](#)

[PDF](#) [Excel](#)

Name	OID	Phone Number	Address	Equipment	Termination Date	Reason for Termination	Last Known Address	Officer / Case Manager
[Redacted]	ID57995	(808) 7210	Bridgeport, CT06605	Not Retrieved - 30+ Days OmniLink (20560027)	Active		CT 06357, USA	
[Redacted]	ID57435	(714) 4832	1220 N Simon Cir, Anaheim, CA92806	Not Retrieved - 30+ Days OmniLink (20454852)	Active		Waterbury, CT 06705, USA	SENTINEL TEST /
[Redacted]	ID57992	(959) 0391	CT06354	Not Retrieved - 30+ Days OmniLink (20426095)	Active		Sprague, CT 06330, USA	
[Redacted]	ID58022	(475) 3670	K5, East Windsor, CT06088	Not Retrieved - 30+ Days OmniLink (20581862)	Active		Enfield, CT 06082, USA	
[Redacted]	ID58025	(646) 2525	Bridgeport, CT06610	Not Retrieved - 30+ Days OmniLink (20091750)	Active		Bridgeport, CT 06607, USA	
[Redacted]	ID57658	(203) 3043	118, West Haven, CT06516	Not Retrieved - 30+ Days OmniLink (20351496)	10/30/2025	Terminated - Violated terms	Hartford, CT 06120, USA	
[Redacted]	ID58014	(203) 3131	Waterbury, CT06704	Not Retrieved - 30+ Days PHMU (710530) Not Retrieved - 30+ Days PTX (210616)	10/30/2025	Successfully Completed		
[Redacted]	ID57981	(347) 9942	Stamford, CT06901	Not Retrieved - 30+ Days PHMU (720267) Not Retrieved - 30+ Days PTX	10/30/2025	Terminated - Violated terms		

The Equipment Retrieval Dashboard also allows agencies to create “phases” associated with recovery efforts, which assists in reducing equipment loss by providing a real-time status for each piece of equipment as updated by the officers. These phases are customizable agency-by-agency just like event/alert notification procedures and allow both Sentinel and agency personnel to follow and record step-by-step instructions throughout the recovery process.

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Participant Information		Equipment		Contacts	
Client:	Tran 12345, Ptran - ID5743390	OmniLink: 20454852	☒ Mark as Retrieved ☐ Mark as Lost	Agency: CTT	
Address:	1220 N Simon Cir, Anaheim, CA 92806			Probation Officer: SSENTINEL TEST	
Home Phone:	(714) 209-4832			Officer Cell Phone: Officer Office phone:	
Cell Phone:	Work Phone:			Officer Email: abyss@sentrak.com	
TimeZone:	PST			Case Manager:	
Start Date: 04/23/2024	Termination Date: Active			CM Cell Phone: CM Office phone:	
Reason				Case Manager Email:	
Comment					

Phase 1 (Contact) Comments: Call the participant at all available numbers within the 1st business day of being deleted. NOTE: If the participant does not have valid number; call or email Assigned Officer requesting a valid number.

Phase Results	Spoke to Participant	Comments
No Actions Found!	Wrong Number/Disconnected Blocked Call No Answer Field Contact	

Each Phase or attempt made to recover a piece of equipment is logged within the Equipment Retrieval Dashboard and the Phase Result is added by the person performing the action. This in turn allows the next Phase of the recovery process to be initiated and follow through all other Phases set up by the agency until the device is either recovered or reported to Sentinel as Lost.

If the device is recovered during any point in the recovery process, the officer can go to the Dashboard, select the participant/device and select the “Mark as Retrieved” button to place the device back into the agency’s inventory and close out the recovery efforts. Once this has been completed, a report can be generated and exported to PDF detailing the Phases utilized in the recovery effort and notes associated with each attempt.

Equipment - ID:

OmniLink

Serial Number: 2004

Disposition: Pending Pickup

Retrieved

Lost

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



OPTIONAL CASE MANAGEMENT MODULE

Unlike other vendors who claim to have a case management system but only have a limited number of fields in their offender monitoring system, Sentinel designed and developed our case management module specifically for these types of programs. Our proprietary web-based information system is designed to be able to handle offender caseloads and all the data and interactions that comprise an offender population. We can track a practically endless amount of data for each offender including:

- + Participant photo
- + Full name and address information (both current and previous residences)
- + Personal information; *i.e.*, Gender, Eye and Hair color, languages spoken, acquaintance information, tattoos or distinguishing body marks (SMTs), aliases
- + Multiple cases (both consecutive and concurrent) present and historical
- + Multiple case numbers
- + Sentence lengths
- + Daily program monitoring fee information
- + Drug Screening
- + Agency information
 - o Court data
 - o Law enforcement or court/probation officer data
 - o Attorney data
- + Employment data
- + Permitted Activities
- + Agency specific tracking data (Booking numbers, "X" numbers, CII numbers)
- + Ability to add additional fields as requested by Agency personnel

In addition to queries, our Active Case Management system can be used to generate the following reports:

- + **Enrollment Notices:** Created when the offender is enrolled in the program.
- + **Completion Notices:** Created when the offender completes the program.
- + **Non-Compliance Reports:** Created for any instance of non-compliance.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **Abscond Reports:** Created for situations when an offender cannot be located due to failure to return to the residence and/or has removed the tracking equipment. Prior to issuing an Abscond, our case managers will have done the necessary research (contacted friends and family, employment sites, and any reasonable alternate contacts to determine the offender's whereabouts).
- + **Termination Reports:** Used when the offender unsuccessfully is removed from the program, including re-arrests or removal by order of the court or other correctional entity.
- + **Status Reports:** Used to report any changes in the offender's status. Also provided as "Progress Reports" when required by Agency personnel.
- + **Schedule Change Reports:** Can be provided to indicate schedule change history.
- + **Court Testimony:** We have program personnel including the Account Manager, as well as corporate personnel that can testify in court.

All our queries and Active Case Management reports can be used to generate comprehensive and all-inclusive reports that can be provided to the Agency at any interval.

More importantly, DNA ensures accurate and consistent posting of payments by utilizing our Automated Payment Application. This application ensures every payment received, whether via credit card, money order, or collections, from the online payment website are appropriately receipted and applied to the participant's account.

The screenshot shows the SENTINEL web application interface. The top navigation bar includes links for Change Group, Select Client, Reports, Report Forms, and Log Out. The left sidebar shows a menu with options like Agency, User, Client Info, Client Cases, and Client Payments. The main content area displays the Client Debit History for MIA_ID00003 Mark Waugh - Miami Dade Miami Dade. It includes a table with columns for Date Applied, Debit Type, Comments, and Amount Due. The table shows five entries for Electronic Monitoring from 2017-05-01 to 2017-05-05, each for \$7.00. Summary rows show Total Debits of \$35.00, Total Payments of 0.00, Balance of \$35.00, and Pay Off Amount of \$933.00.

Date Applied	Debit Type	Comments	Amount Due
2017-05-05	ELECTRONIC MONITORING		\$7.00
2017-05-04	ELECTRONIC MONITORING		\$7.00
2017-05-03	ELECTRONIC MONITORING		\$7.00
2017-05-02	ELECTRONIC MONITORING		\$7.00
2017-05-01	ELECTRONIC MONITORING		\$7.00
Total Debits			\$35.00
Total Payments			0.00
Balance			\$35.00
Pay Off Amount			\$933.00

MOBILE APPLICATION

The **DNA Mobile Application** is designed for officer use and to streamline feature sets that are available in our full featured DNA website. The abbreviation of certain features and the addition of others in the DNA Mobile App will improve the mobile access experience of our customers using smartphones and tablets. The features of DNA Mobile App were created using valuable input from a panel of supervising officers who routinely work remotely and away from their office. DNA Mobile App facilitates remote supervision like no other and is a valuable tool in the participant supervision process.

Free to our customers, our DNA Mobile App is available for download at the Apple App and Google Play Stores. Compatible with iOS and Android OS, DNA Mobile App utilizes TLS 1.2, AES-256 encryption to ensure all customer and participant data is secure. The DNA Mobile App features:

- + **GPS Mapping:** View GPS tracking history, Current Location, and Zones via DNA Mobile.

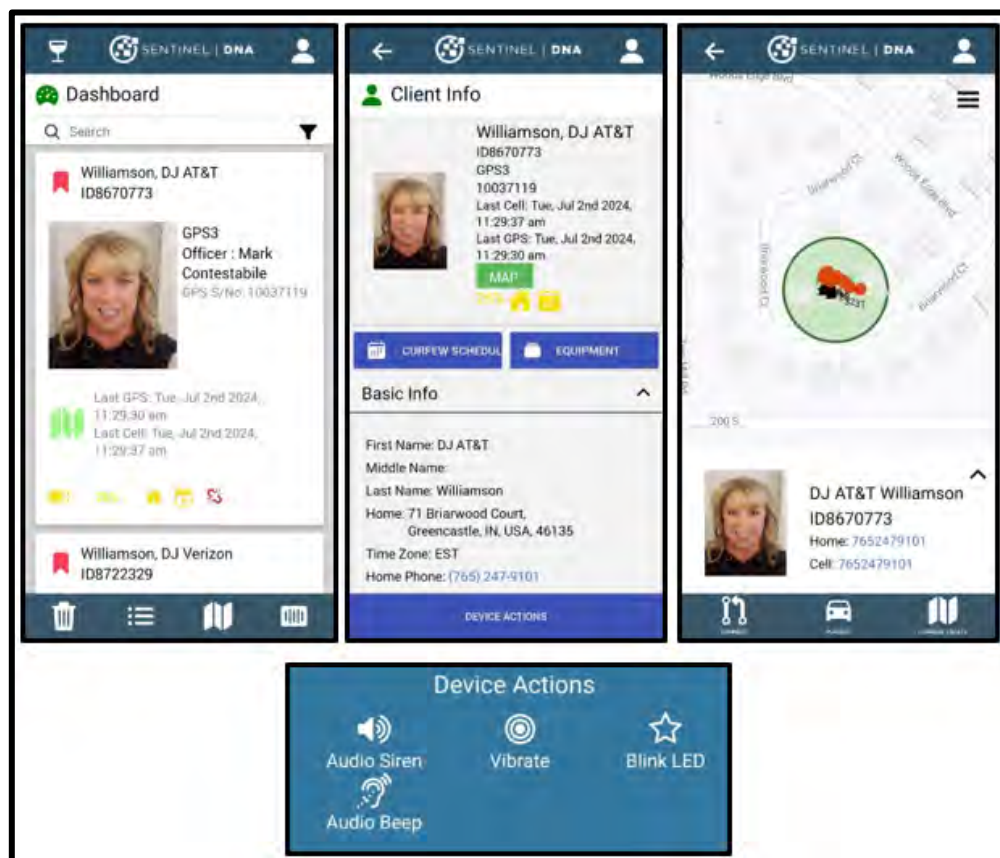
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



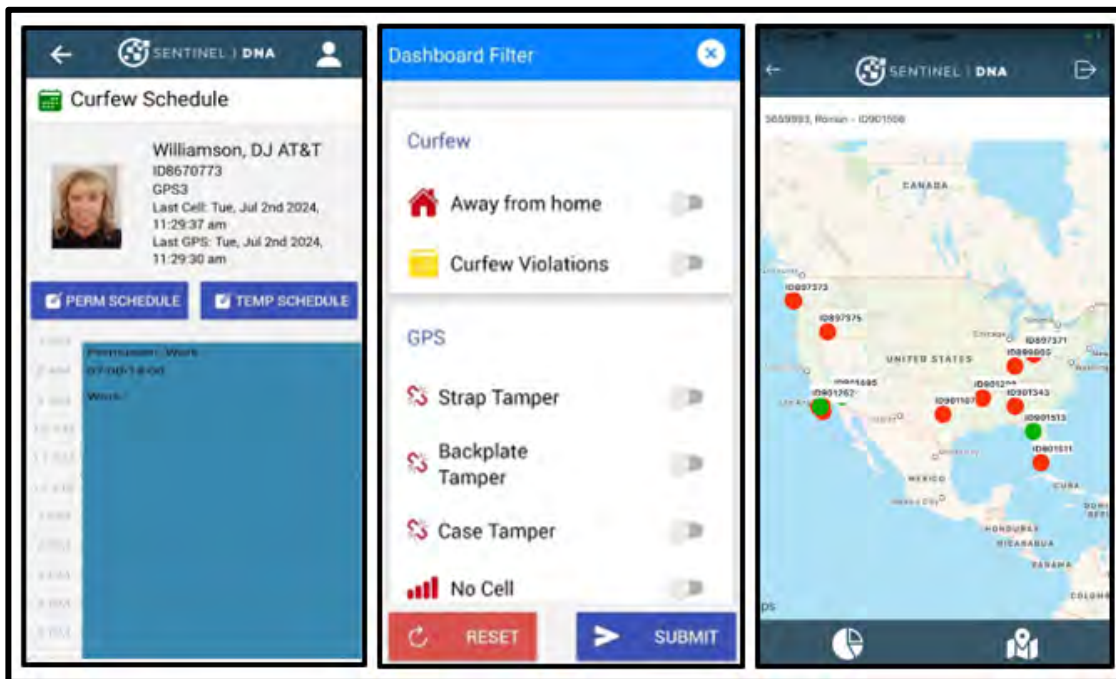
- + **View and Edit Participant Information:** Modify Participant Name, Device ID, Case Information, Home Address, etc.
- + **Alert Resolution:** View, Respond and Clear Alerts directly from DNA Mobile.
- + **Scheduling:** Quickly update a Participant's Curfew/Home Zone Schedule.
- + **Notify Participant:** Easily send commands to the GPS device.
- + **Initiate a Field Contact:** Verify and document field contacts with participants while using DNA Mobile App to record the date, time, location, and notes for each contact.
- + **Profile Photograph:** Update participant photos directly through DNA Mobile App.
- + **Travel Directions:** Provides turn-by-turn directions from officer's location to the last known location of the participant or selected address.
- + **Activity Review:** Quickly review all participant activity from GPS and Radio Frequency (RF) devices via DNA Mobile App.
- + **Pursuit Mode:** Initiate Pursuit Mode to activate faster GPS acquisition and reporting.
- + **Inventory:** Easily identify inventory availability and status.

The images below display some of the valuable features within our DNA Mobile App.



Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SMARTPHONE APPLICATIONS

ADVOCATE™, VICTIM NOTIFICATION AND TRACKING APP

Combining a Victim's smartphone with the advanced tracking capabilities of Sentinel's OM500 GPS device, Advocate allows law enforcement and corrections agencies to track and compare location data of participants and Victims of domestic violence simultaneously through Sentinel's proprietary DNA monitoring system.

Advocate™ Victim Notification Application is compatible with Apple OS, Android OS, and/or Windows-based devices and specifically designed to provide a more efficient and convenient alternative for domestic violence cases. As an alternative to victims carrying a secondary GPS device, Sentinel has developed our Advocate, Victim Notification and Tracking Application, that will enable configuration of a Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilize the victim's smartphone to acquire and report GPS data to our DNA monitoring system that will compare the victim's location to the offender's location. In the event the participant attempts to remove the GPS tracking device or violate any restrictive zone, the victim will receive the notification on her/his personal cellular device. It also allows tracking of the participant and his/her location compared to the victim to reduce the chance of an encounter while in the community. Advocate has been designed to provide notification to the victim and will also:

- + Provide alerts/violations about the offender's device to the victim's smartphone, which can be configured by the agency
- + Allow the victim to Dial 911 within the App



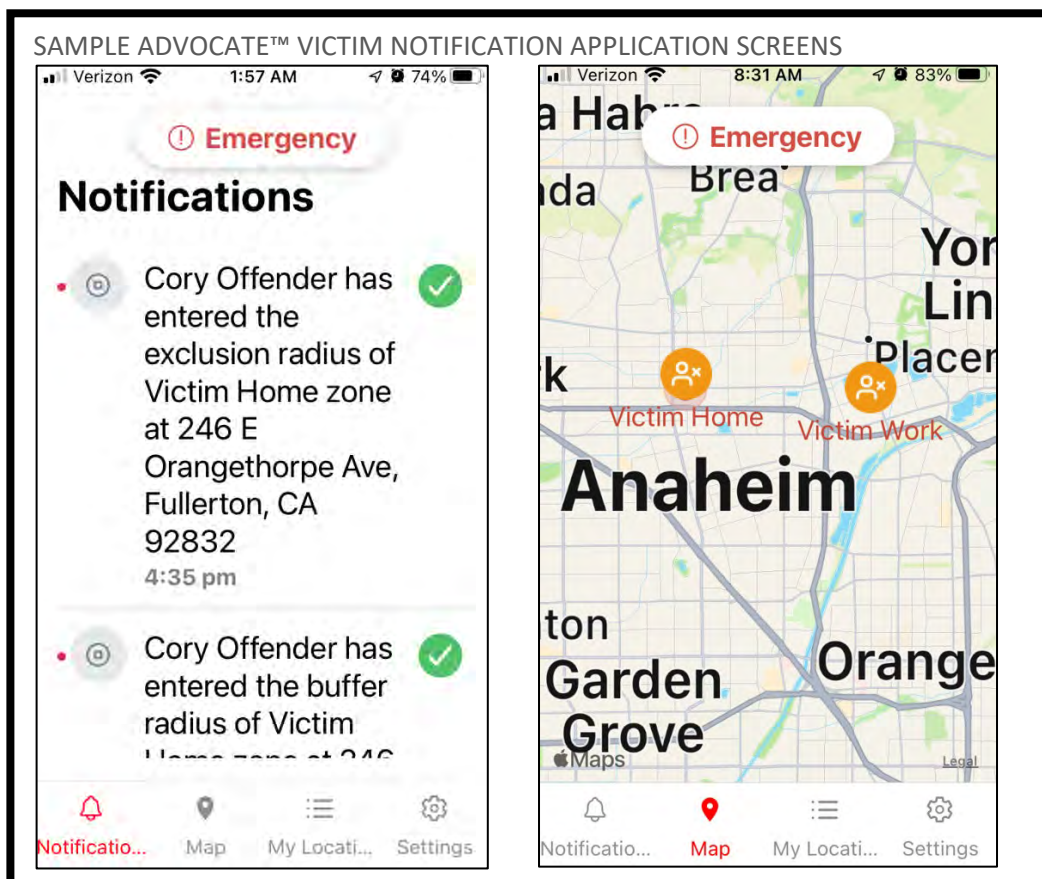
**Request for Proposals for
ELECTRONIC MONITORING**

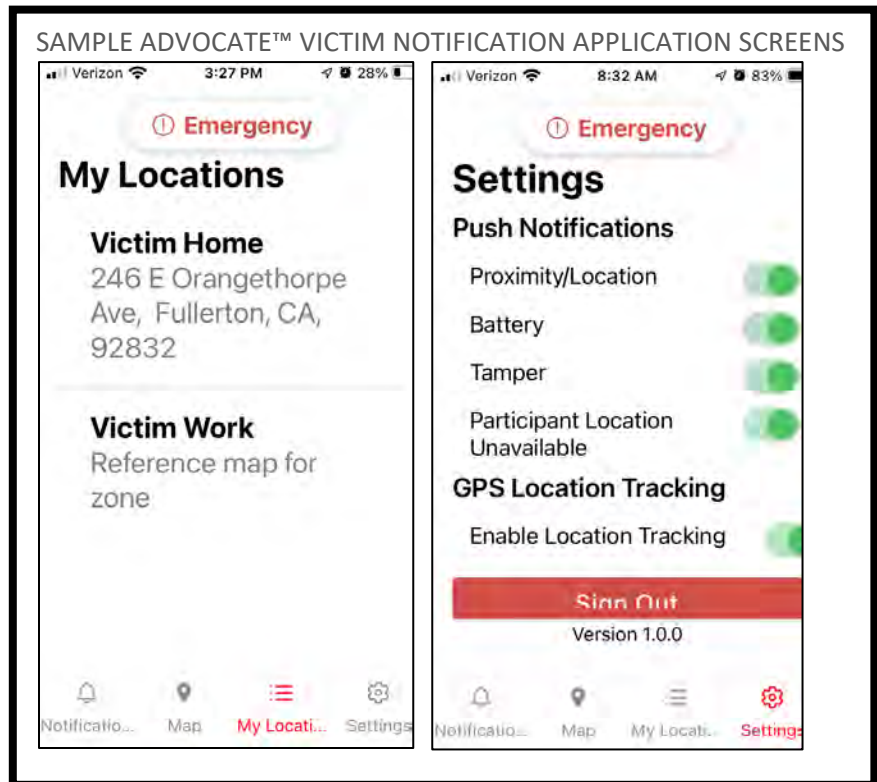
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Allow the victim to access support telephone numbers such as the Victim Advocate Office, the Prosecutor's Office, and/or the agency's office
- + Display established exclusion zones associated with the participant
- + Enable Push Notifications of participant non-compliance to the victim
- + Allow the victim to receive push notifications from SentinelDNA when the Victim App has been disabled, thereby notifying the victim that their location services are disabled and thus no longer tracking their proximity to the participant

As an alternative to victims carrying a secondary GPS device, Sentinel's Advocate will enable configuration of a Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilize the victim's smartphone hardware to acquire and report GPS data to the DNA monitoring system that will compare the victim's location data to the participant's location data. Please refer to the examples of sample screens below for Advocate.





PARTICIPANT COMPANION APP

Sentinel is proud to announce the upcoming release of our latest addition to the SentinelDNA monitoring system and our newest and most innovative smartphone application, the Participant Companion App.

Designed to reduce the number of program alerts and improve communication between the officer/participant while simultaneously improving officer efficiency, the optional Participant Companion App works in conjunction with our SentinelDNA monitoring system and will provide participants with the ability to submit permanent and temporary schedule requests for GPS and/or radio frequency monitoring, upload documents, and "Chat" with their assigned case manager/officer. The Participant Companion App will be available in Q2-2026 for iPhone, Android, and Windows-based smartphone devices for participants designated within their SentinelDNA profiles for app usage. The App can be downloaded onto the Participant's smartphone.

The SentinelDNA monitoring system will provide visual indicators or icons on the Dashboard allowing authorized agency personnel to quickly see pending schedule requests, unread chats and unread document uploads. Authorized users will also be able to click on the icon in order to access the pending items and 1) review, approve, modify and approve, or deny schedule requests; 2) review uploaded documents and save them to the participant's DNA record; and 3) engage in an in-app chat with the participant or multiple participants simultaneously. Agency personnel will also be able to receive real-time notifications via email/text for pending schedule requests and uploaded documents.

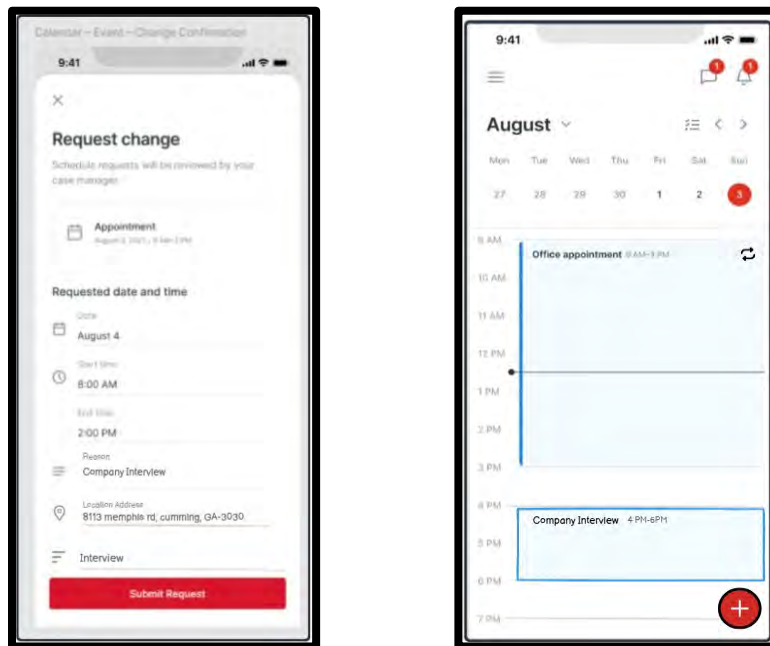
Scheduling Changes Feature. The Companion App will include a feature that allows the participant to request schedule changes directly through the App. The officer will have visibility on this request through DNA and will be able to approve or deny the request with a simple mouse click. If the schedule is approved, it will be automatically delivered to the DNA monitoring system allowing the schedule to change without any further officer interaction. All approvals/denials are communicated back to the participant via the Companion App with all interactions between the officer and the participant captured with DNA.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The Participant Companion App will display the participant's current schedule in the app calendar at all times thereby reducing compliance alerts from the client "forgetting" their schedule. The client will submit schedule requests through the calendar and if approved by their assigned case manager/officer, they will receive notification of the approval along with the new event loading into the calendar. This will allow participants to always have access to their current, approved schedule.



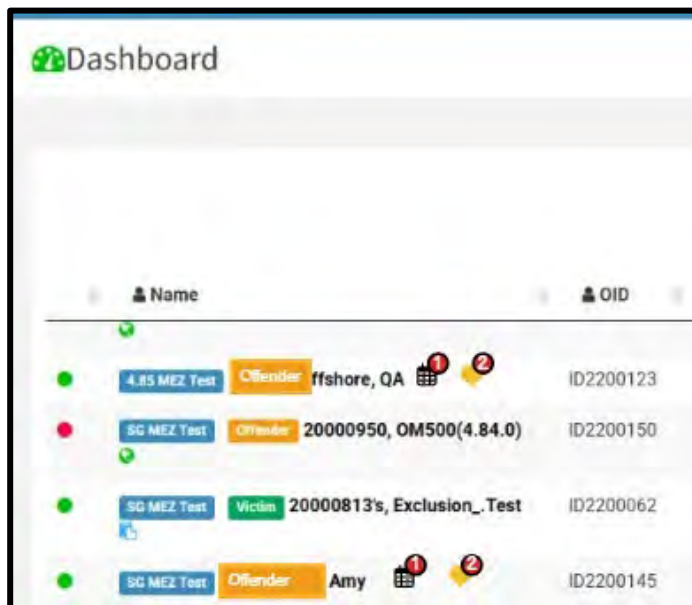
Chat Feature – Participant / Officer Communications. The Companion App also includes the release of a "Chat Feature" that will allow the officer and participant to communicate via chat with all interactions captured and stored in the DNA system for future reference. This feature allows clients to ask quick questions or report issues without waiting for an office visit or playing "phone tag" with the officer, reducing the risk of accidental non-compliance due to miscommunication.

Document Upload Feature. The Companion app will allow the participant to upload required documents, court orders, verification confirmation, etc. directly into the DNA monitoring system via the Companion App. This feature will allow participants to submit required documents to their supervising officer 24/7 without being required to report in person to the office resulting in higher compliance rates by minimizing the time and effort required from the client..

The officer is provided with icons that clearly indicate a client's submitted schedule change request as well as conversations via the chat feature that need to be addressed. The Companion App has been designed to reduce the number of alerts as client schedules are processed immediately upon approval thus reducing the amount of curfew related alerts.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

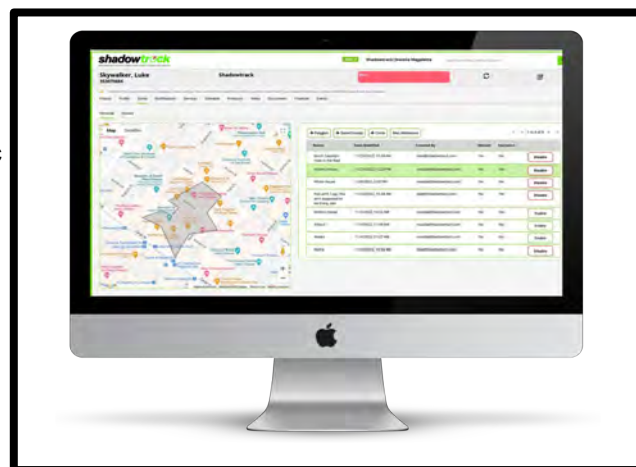


The features associated with the Participant Companion App can be added or removed on a participant-by-participant basis thus allowing officers/case managers control over which features are available to each individual participant.

SHADOWTRACKONE MONITORING SYSTEM (OPTIONAL)

The ShadowtrackONE platform is robust and user-friendly allowing access over a wireless network 24 hours per day, 365 days per year without interruption. Whether the participant is installed on App Related Services, GPS Tracking Devices, or a combination of technologies, the basic functionality of the system remains the same and everything is easily accessible in one complete software package that is viewable via a desktop computer or mobile application. Key features include:

- + GPS, Alcohol, and App Services in Single Database
- + Enhanced Mapping Capabilities
- + Real-Time & Historical Data
- + Automated Monitoring Functions
- + Report Options
- + 24/7 Access
- + Multilingual
- + 2-Factor Authentication



Dashboard Features

Upon logging into the system, authorized users are immediately taken to the ShadowtrackONE dashboard screen which displays all program participants, as well as alarm details, last known tracking points, device type, etc. This data can be filtered by All Active Participants and/or only by those assigned to an officer's caseload. A map can be displayed showing all active program participants' locations on a single map allowing agency supervising personnel to quickly ascertain if any participants are in or out of program compliance. The Dashboard also

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



contains an Officer's Portal in which App Related Functions can be performed. Whether agency personnel want to place a video call with a participant, perform an On-Demand Location Check, perform a Secured Chat Session with a participant, send a Mass Notification message to all participants, etc.

Enrollee	Enrollee ID	Assigned Officer	Alarms	Info
Demo (Ankle), McAndrew	521533460	McAndrew, Tom (Shadowtrack)	2 Alarm(s) Protocol: McAndrew Agency Device Protocols	ShadowDevice Battery: 94% Last Comm: 8/19/2024, 1:02 PM
Demo (ShadowPhone/Tether), McAndrew	521546726	McAndrew, Tom (Shadowtrack)	1 Alarm(s) Protocol: McAndrew Demo (ShadowPhone)	ShadowPhone Battery: 75% Last Comm: 8/19/2024, 1:00 PM
Demo (Watch), McAndrew	521545226	McAndrew, Tom (Shadowtrack)	2 Alarm(s) Protocol: McAndrew Agency Watch Protocols	Mobile Without App ShadowWatch Battery: 87% Last Comm: 8/19/2024, 1:00 PM

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Participant Profiles (Accessing and Adding Profiles)

It is extremely easy to access or add participant profiles in our monitoring database. To access an existing participant profile, simply click on the individual's name on the Dashboard or an authorized user can access this information by clicking on the Participant icon in the left portion of the screen which displays various menu items. Once selected, the officer will see all the pertinent information as it pertains to the individual participant.

The screenshot shows the Shadowtrack web application interface. On the left is a green sidebar with navigation icons. The main content area is titled "shadowtrack" and "Shadowtrack | McAndrew, Tom (Shadowtrack)". Below the title is a search bar and a navigation menu with options: History, Profile, Zones, Notifications, Services, Schedule, Protocols, Notes, Documents, Financial, and Check-Ins. The "Profile" tab is selected, showing "Basic Information" and "Details" sections. The "Basic Information" section includes fields for First Name (McAndrew), Middle Name, Last Name (Demo (Watch)), Suffix, Internal ID, Primary ID, and Image. The "Details" section includes fields for Email Address, Date of Birth (12/14/1972), Language (English), Time Zone ((GMT-05:00) Eastern/US), Address (224 Dunbar Drive, Mechanicsburg PA 17050, United States), and Assigned User(s) (McAndrew, Tom (Shadowtrack)). An "Edit" button is located at the top right of the "Basic Information" section. The "Details" section has tabs for "Enrollment", "Phone", and "Cases". The "Enrollment" tab is active, showing fields for Active (Yes), Active Start Date (11/11/2023, 5:00 PM), Active End Date, Enrollment Password (7084212), Date of Voice Enrollment, Date of Facial Enrollment, and TFN Opt Out Date. There are buttons for "Show History", "Update Active Dates", "Reset Enrollment", and "Enrollment Form".

Inclusion/Exclusion Zones

Agency staff can easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones are automatically created around the borders of the desired States or Counties. Zones can be created specifically for an individual participant or shared between multiple participants.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack | McAndrew, Tom (Shadowtrack)

Search enrollees, entities & users

Map Satellite

Zone Name

Massachusetts Probation

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

Street

1 Ashburton Place

Unit

Room 405

City

Boston

State

MA

Zip Code

02108

Country

United States

Find Location

Center

(42.35990412639689, -71.0623588005265)

Radius (ft)

374.06

MAC Address

Save Cancel

shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack | McAndrew, Tom (Shadowtrack)

Search enrollees, entities & users

Map Satellite

Zone Name

Massachusetts

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

State-wide

Massachusetts

County

MAC Address

Save Cancel

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Schedules

Once a zone is set up, schedules can be easily entered to designate the time a participant should or should not be in during specific times, days of the week, etc. Schedules are first set up by determining the zone type; Inclusion (a place they are supposed to be) or Exclusion (a place they are prohibited from being), then select the zone from the dropdown menu. A start date and time can be specified or the all-day option can be toggled on. The recurrence is determined by selecting from the drop-down menu: Never, Daily, Weekly, Every Week Day, Monthly. Schedule Exceptions can be added to permanent schedules for one-time occurrences (i.e. doctor appointments, court proceedings, etc.). Additionally, a zone can be set up around the entire state or county to alert supervising staff if any program participants leave the state or county without prior permission.

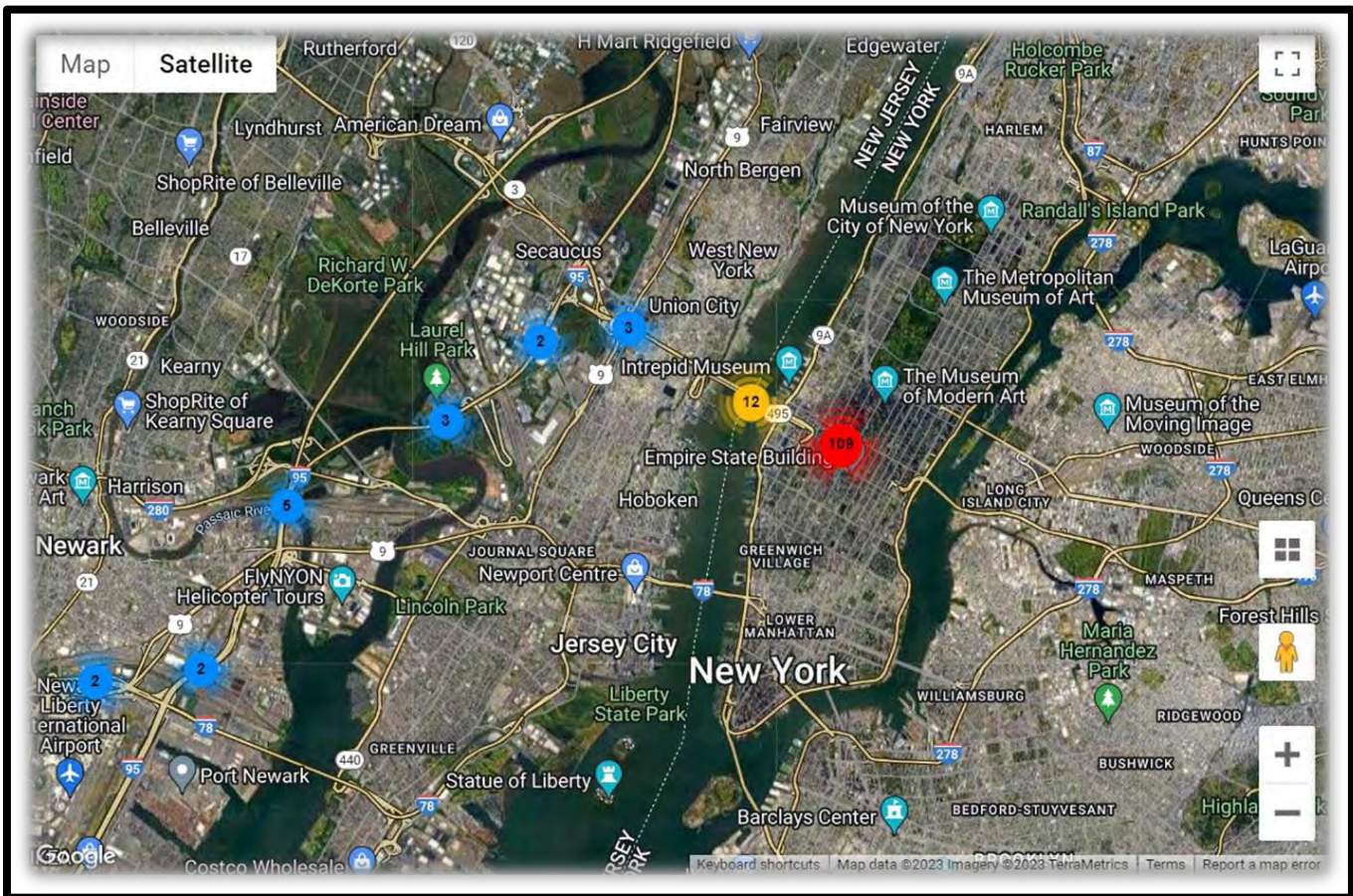
Type	Starts On	Recurrence	Zone Name
Inclusion	11/11/2023	Daily	Home
Exclusion	12/4/2023	Daily	Maury County Sheriff's Office

Tracking Details

Tracking data is achieved through the ability of the ShadoWatch device to obtain location through GPS Satellite data and Wi-Fi data, as well as Location Base Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the device is in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS nor Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located. Additional details such as battery percentage, speed of travel and direction of travel are also displayed. The mapping function allows an agency to filter tracking data by specific date and time periods and offers an automatic playback feature when reviewing tracking data.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Date Range
Custom

Filter Start (User Time)
12/10/2023 2:00 PM

Filter Start (Enrollee Time)
12/10/2023, 2:00 PM

Export

Maximum 250 locations displayed

Filter End (User Time)
12/10/2023 5:00 PM

Filter End (Enrollee Time)
12/10/2023, 5:00 PM

Recent

1 to 5 of 173

1	12/10/2023 04:59 PM EST	Address	GPS Speed: 38.66	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
2	12/10/2023 04:57 PM EST	Address	GPS Speed: 37.48	Battery: 80 Charging: No Signal Strength: 66 Zone Status:
3	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
4	12/10/2023 04:56 PM EST	Address	GPS Speed: 40.09	Battery: 81 Charging: No Signal Strength: 66 Zone Status:
5	12/10/2023 04:55 PM EST	Address	GPS Speed: 33.37	Battery: 81 Charging: No Signal Strength: 66 Zone Status:

PRIORITY COMMUNICATION

The OM500 device ensures continuous communication of location data by prioritizing GPS satellite tracking and automatically transitioning to alternative location methods when GPS data is unavailable. Location points are first obtained via GPS satellites based on the device's rate plan. If GPS points cannot be obtained, the device automatically switches to Wi-Fi-based location data, and if neither GPS nor Wi-Fi is available, cellular cell-tower scan location points are generated. Location data is processed through a third-party provider to determine position and accuracy, ensuring uninterrupted location reporting during high-traffic periods and critical situations.

The OM500 is the most advanced one-piece GPS Offender Tracking and Location Monitoring unit in the industry that reliably communicates monitoring and location data over the Verizon LTE or AT&T LTE networks including all roaming partners. To ensure continuous communication of location points in high traffic times and critical situations, the OM500 supports, and Sentinel is approved for, activation for its OM500 GPS devices on Verizon's Frontline network that prioritizes communications and delivers enhanced connectivity during high traffic times and critical situations. With this approved capability from Verizon, the OM500 is equipped to provide NASPO ValuePoint Participating Entities continued and reliable communications during critical situations and emergency conditions. With tens of thousands of devices communicating daily Sentinel has not seen nor been subject to high traffic delays even during critical situations such as hurricanes or fires.

Further, the OM500 device incorporates advanced technologies and methods to ensure that tracking and location monitoring points from an entity program participant wearing an OM500 device accurately and continuously reports location data, through the following advance technological methods.



- + **Zones On Board.** The OM500 incorporates smart device technology that allows for GPS-based **zones “on board”** whereby, the device will immediately report zone violations and tamper alerts immediately in high traffic times and critical situations. This method is far superior to other providers who store zones on the monitoring application and cannot immediately report key alerts.
- + **Pursuit Tracking Mode.** For situations where officers are trying to pursue a GPS participant in real-time, our Pursuit Mode feature allows for the capture of a GPS location every fifteen (15) seconds and report every (30) seconds allowing for real-time tracking capability. This feature can be initiated by Department officers, Sentinel personnel, or by our National Monitoring Center if requested by Department officers while in pursuit. Pursuit Mode tracking can be initiated from any internet accessible device through our web-based Sentinel monitoring system as well as from any mobile device through our Mobile App.
- + **Industry Leading Triple Tracking Capability via GPS, Wi-Fi location Points, and Cellular Tracking.** The OM500 leverages three (3) industry-leading location-based services provided by Skyhook. This hybrid Precision Location system locates our devices using GPS, Wi-Fi and cell signals ensuring that all devices can be accurately located in virtually every environment, including high traffic times and critical situations. In impaired areas where GPS alone cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. **This allows for a significantly more robust device as it offers multiple tracking options.**
- + **Triple Tamper Detection including: 1) fiber-optic strap design strap tamper; 2) device case tamper; and 3) backplate tamper.** Within seconds the OM500 generates a tamper alarm in the event an offender is tampering with the equipment. Using a combination of fiber optics within the strap and dual pressure sensors within the device, *the OM500 device automatically and instantly communicates to the monitoring system when a participant attempts to remove the device or tampers with the strap.* The OM500 device will send a tamper alert if the participant severs the strap or if the unit loses contact with the backplate, indicative that the device has been uninstalled/disassembled. Additionally, the unit will send a tamper alert if the unit is broken/cracked or if the unit’s backplate is separated from the rest of the device.

The above advanced features ensure continuous communication of location points in high traffic and critical situations.

4. Describe the alerts that can be set up (location, time constraints, tamper alerts, low battery, etc.). Describe the process for setting system alerts for violations (curfew, zone, tamper). Include the alert intervals and how long it will take for the hardware to communicate with the software. Describe how the technology reduces false tampers and ensures accurate alert notification.

SENTINEL RESPONSE

OM500

Sentinel's OM500 GPS tracking device is the most advanced one-piece unit in the electronic monitoring industry today. Our state-of-the-art device incorporates a rugged and durable Acrylonitrile-Butadiene-Styrene (ABS) Plastic casing that is ultrasonically welded resulting in a hardened and waterproof design that can withstand temperatures between -4° Fahrenheit and 140° Fahrenheit and submersion to a depth of one (1) atmosphere, or 33 feet, in both salt water and fresh water. The OM500 also incorporates a hypoallergenic strap made of Thermoplastic Polyurethane which is designed with embedded fiber optic lines and is securely attached to one side of the device with security screws prior to shipment. These enhanced design features of the OM500 eliminate failure points seen with other devices in the industry and in turn, minimize nuisance and/or false alerts such as device tampers and strap tampers.



In addition to its ruggedized construction, the OM500 boasts the industry's longest battery life exceeding five (5) days from a single charge. This extended battery life reduces the incidence of low battery alerts and allows agency personnel to focus on supervision. The OM500 also incorporates quick charge technology thus only requiring a charge time of thirty (30) minutes if charged on a daily basis. In the event the OM500 is not charged according to instruction, it incorporates an additional safety and performance feature whereby it generates two (2) separate low battery alerts. The first low battery alert occurs when the device reaches approximately 30% remaining battery life, while the second low battery alert occurs when the OM500 reaches 20% or less remaining battery life. These percentage thresholds are customizable thus allowing agency specific percentages to be established if required.

To aid agency personnel with a real-time response to curfew and zone violations, the OM500 is equipped with onboard, non-volatile memory allowing the storage of zones onboard the device. This onboard zone storage allows the OM500 to initiate immediate notifications of zone crossings for Home Zones and other types of Inclusion Zones. Each exit from, and entry to, the Home Zone or Inclusion Zone is reported by the GPS unit to our SentinelDNA web-based monitoring system immediately and is compared to the permitted schedule. Any discrepancies between the time of zone entry/exit with the permitted schedule will generate an alert based on the agency's established notification parameters. This activity verification is continuously performed by DNA ensuring proper monitoring of each program participant and accurate alert notification to agency personnel.

In addition to the onboard storage of Home Zones and other types of Inclusion Zones, the OM500 also stores Exclusion Zones on board the device allowing for immediate notification of entry and exit alerts to agency personnel. As an added Sentinel advantage, when the OM500 enters a designated Exclusion Zone, the device increases the acquisition and transmission of its tracking data receiving updated locations every fifteen (15) seconds and transmitting the location data every thirty (30) seconds. This increased acquisition and transmission of location data provides additional tracking information which in turn allows for a more rapid response by agency personnel to these exclusion zone alerts. In normal operating conditions (cellular availability) the OM500 communicates with the software in near real-time (within 1 minute) through the cellular network.

Sentinel DNA Profile Manager

Sentinel's DNA web-based monitoring system allows agencies the ability to set up custom notifications for **all** identified key events/alerts by using the DNA Profile Manager. **Each alert notification can be set up for immediate delivery or set up with an agency established grace period or hold time prior to delivery.** Notifications can be sent to individual officers or to multiple agency personnel simultaneously, and delivery is available through multiple communication methods, including text message, email, automated voice message, telephone call and web-based report review. The DNA Profile Manager allows agencies to set up automated notification and optional manual escalation/closed loop notification and sequencing. Agencies also can differentiate protocol changes within a single alert by time and day of the week providing versatility and customizable responses. Agencies can establish multiple notification profiles allowing for distinct protocols and procedures for specialized populations and/or individual participants.

To aid agency personnel with a real-time response to curfew and zone violations, the OM500 is equipped with onboard, non-volatile memory allowing the storage of zones onboard the device. This onboard zone storage allows the OM500 to initiate immediate notifications of zone crossings for Home Zones and other types of Inclusion Zones. Each exit from, and entry to, the Home Zone or Inclusion Zone is reported by the GPS unit to our SentinelDNA web-based monitoring system and is compared to the permitted schedule. Any discrepancies between the time of zone entry/exit with the permitted schedule will generate an alert based on the agency's established notification parameters. This activity verification is continuously performed by DNA ensuring proper monitoring of each program participant and accurate alert notification to agency personnel.

In addition to tamper alerts (strap, backplate, device, and slippage), low/dead battery alerts, and zone alerts (home, inclusion, stationary exclusion, mobile exclusion, and buffer), DNA's Profile Manager includes alerts for loss of device communication, loss of GPS signal, and potential device shielding. As a unique and added Sentinel

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



advantage, our Profile Manager affords agencies the ability to establish reminder alerts associated with key events such as being away from the Home Zone for extended periods of time outside of the approved schedule as well as continued losses of communication and/or GPS signal and ongoing instances of a dead battery. These reminder notifications are available at additional one (1) hour intervals up to and including 24 hours and then if unresolved, would repeat every 24 hours thereafter. The ability to include these additional notifications for key events allows agencies to ensure resolution regardless of possible staffing shift changes that may occur or accidental clearing by an individual officer/case manager prior to full alert resolution.

Prior to deployment of Sentinel devices, authorized agency administrators will work with Sentinel's specialized Help Desk Technicians and Field Operations personnel to determine the required profiles and individual events for each profile that best suits the program's target population(s). Our Help Desk will then build the profile(s) based on the approved protocols and then work with agency administrators to ensure success deployment and ongoing needs should they change.

Below is a list of available events/alerts that can be included within the notification profile(s).

UNAPPROVED LEAVE	LATE TO ENTER
UNSCHEDULED LEAVE	FAILED TO ENTER
FAILED TO LEAVE	UNAPPROVED ENTER
NO RETURN 2 HOURS / 4 HOURS / 12 HOURS / 24 HOURS	
INCLUSION ZONE ENTERED	INCLUSION ZONE CLEARED
LATE TO ENTER INCLUSION ZONE	FAILED TO ENTER INCLUSION ZONE
UNAPPROVED INCLUSION ZONE ENTERED	UNAPPROVED INCLUSION ZONE CLEAR
EXCLUSION ZONE ENTERED	EXCLUSION ZONE CLEARED
BUFFER ZONE ENTERED	BUFFER ZONE CLEARED
GPS LOW BATTERY	GPS LOW BATTERY CLEAR
DEAD BATTERY	DEAD BATTERY CLEAR
DEAD BATTERY 2 HOURS / 4 HOURS / 8 HOURS / 12 HOURS / 24 HOURS / 24+ HOURS	
NO GPS 1 HOUR / 2 HOURS / 3 HOURS / 4 HOURS / 8 HOURS / 12 HOURS / 24 HOURS / 24+ HOURS	NO GPS CLEAR
NO GPS - NO CELL 1 HOUR / 2 HOURS / 3 HOURS / 4 HOURS / 8 HOURS / 12 HOURS / 24 HOURS / 24+ HOURS	NO GPS – NO CELL CLEAR



POTENTIAL SHIELDING	POTENTIAL SHIELDING CLEAR
POTENTIAL SLIPPAGE	POTENTIAL SLIPPAGE CLEAR
BACKPLATE TAMPER	BACKPLATE TAMPER RESET
DEVICE CASE TAMPER	DEVICE CASE TAMPER CLEAR
XMTR TAMPER – GPS (STRAP)	XMTR TAMPER – GPS CLEAR (STRAP)

SHADOWWATCH (OPTIONAL)

The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the agency's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing enrollee access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

Alert Management Through Monitoring System. Agencies configure alert rules for ShadowWatch violations including curfew violations, zone alerts, tampers, communication interruptions, and battery-related issues through the monitoring platform. Supervising officers can manage all ShadowWatch alerts through the ShadowtrackONE monitoring platform, which allows them to:

- + Review, resolve, and organize alerts by type, client, or caseload
- + Access detailed event data including photographs, GPS points, and testing sequences
- + Initiate on demand tests in response to alert activity
- + Initiate Value-Added Optional Check in Capability
- + Initiate Value-Added Optional Location Based Monitoring of Locations
- + Initiate Value-Added Optional Creation of Inclusion Zones and Exclusion Zones
- + Initiate Value-Added Optional Face Time Video Conference
- + Assigning alert recipients by role or caseload
- + Choosing between real-time notifications or grouped alert summaries
- + Setting zone parameters, schedules, and notification protocols

This flexibility enables agencies to align alert protocols with programming policy.

Alert Intervals and Communication Timing. Shadowtrack is designed for real-time reporting:

- + Each GPS point, BAT test, and facial authentication result are transmitted immediately in accordance with agency protocol standards when cellular and/or Wi-Fi service is available
- + Device-initiated call back frequencies ensure constant communication through the cellular network

The ShadoWatch device can be set to various tracking intervals including 1-minute location intervals and 5-minute location intervals based upon the Participating Entity's desired preference and location data will be reported to the ShadowtrackONE monitoring platform. The ShadoWatch is equipped with multiple location technologies. Tracking data is achieved through the ability of the device to obtain its location through GPS



Satellite data and Wi-Fi data, as well as Location Based Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the devices are in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS or Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located

Zones: Agency staff can easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones are automatically created around the borders of the desired States or Counties. Zones can be created specifically for an individual participant or shared between multiple participants.

Notifications for the ShadoWatch include:

- + Device Communication Timeout
- + Device Communication Timeout Escalated
- + Failed To Charge
- + Band Tamper
- + Within Exclusion Zone
- + Outside Inclusion Zone
- + Lack of Motion
- + Battery Critical
- + Proximity Tamper (No Heart Rate)
- + No Location

5. Describe the process for how you set up maps (e.g. exclusion zone, customizable, pre-loaded?)

SENTINEL RESPONSE

OM500

Authorized users will have access to create, edit, and delete exclusion and inclusion zones for participants being tracked via the GPS tracking device. **SentinelDNA allows for a virtually unlimited amount of exclusion and inclusion zones per participant.** For participants with challenging zones, DNA is also configured to support construction of customizable 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 monitor the movement of the individual program participants.**

Zones can be created as an individual zone, if only one participant will need to use the zone, or as a template zone that can be created and stored within the system as a library of zones if there are multiple participants who need to use the same zone. **DNA allows for the creation of template zones that can be used across a specific population of participants.** This allows agency personnel to designate certain sites across a region as exclusion zones for an entire population of multiple participants. This eliminates the need to repeatedly re-create the same zones for all the individuals identified in a specific population. This type of **template zone** set-up can be used for sex offenders and other high-risk participant populations establishing zones around schools, playgrounds, or related areas of concern.

Zone Options allows supervising entities to view or hide circle and/or polygon template zones on the map, view or hide location labels and zone pins, or re-center the map to a specific address.



Creating a New Circle Zone

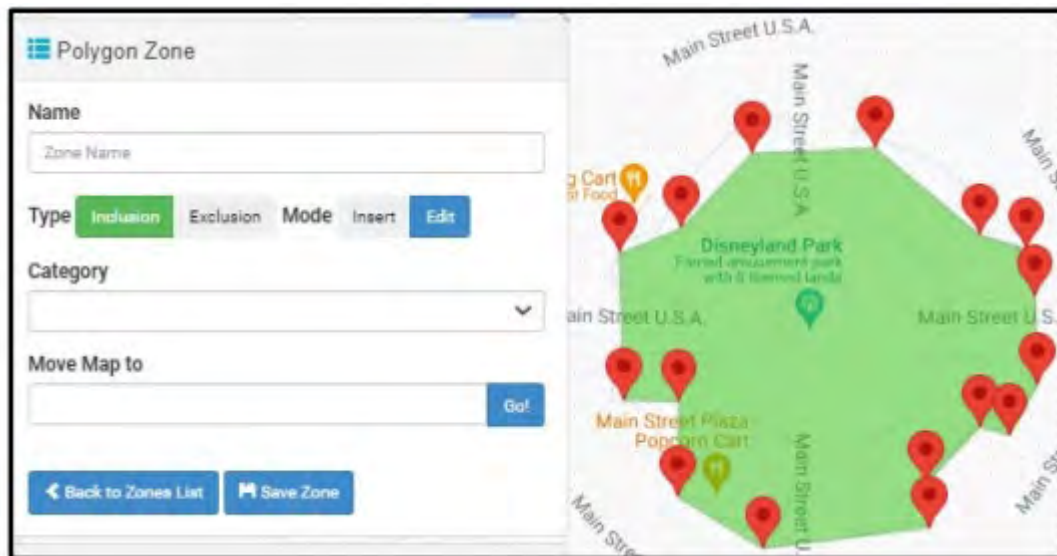
- 1) Select 'New Circle Zone'.
- 2) **Name the zone.** IMPORTANT: If creating a zone for the participant's residence, the zone must be named "Home" to associate the zone with the participant's curfew schedule. A "Home" zone should NOT have a zone schedule. Instead, the Home zone will exclusively rely on the participant's curfew schedule.
- 3) **Radius:** Select the size of the zone (measured in feet).
- 4) **Inclusion or Exclusion:** Select Inclusion if the participant is allowed to enter the zone. Select Exclusion if the participant is not allowed to enter the zone.
- 5) **Latitude and Longitude:** This will auto-populate after entering an address and selecting Move to this address.
- 6) **Street:** The circle zone will default to the home address of the participant. To change the address and move the zone to another location, enter the new address and select "Move to this address."
- 7) **Category: Label the zone.** This feature is optional and is used for informational purposes only.
- 8) Select 'Save Zone' to save the newly created zone.
- 9) Select 'Back to Zone List' to return to the zone list after creating the new zone.

A screenshot of a web form titled "Circle Zone". The form includes fields for "Name" (with a placeholder "Zone Name"), "Radius" (set to 300 feet), "Buffer" (set to 0), "Inclusion" (selected) and "Exclusion" buttons, "Latitude" (43.5978193) and "Longitude" (-116.6458923), "Street" (1290 N Hancock St), "City" (Anaheim), "State" (California), "Zip" (92807), and "Country" (USA). There is a "Category" dropdown menu and a "Send Zone to Device" checkbox. At the bottom are buttons for "Back to Zones List", "Move to this address", and "Save Zone".

Users can manually adjust the position of the zone, click the red zone marker icon and drag the zone to the correct location.

Creating a New Polygon Zone

- 1) Select 'New Polygon Zone'.
- 2) **Name the zone.** IMPORTANT: If creating a zone for the participant's residence, the zone must be named "Home" to associate the zone with the participant's curfew schedule. A "Home" zone should NOT have a zone schedule. Instead, the Home zone will exclusively rely on the participant's curfew schedule.
- 3) **Type:** Select Inclusion if the participant is allowed to enter the zone. Select Exclusion if the participant is not allowed to enter the zone.
- 4) **Insert Mode:** Select Insert as the mode to create the outline of the zone by clicking on the map to place markers that represent the corners of the zone. A minimum of three or as many as 16 markers can be created. NOTE: After a marker has been placed, it can be repositioned by dragging it with the cursor. Double-click on a marker to remove it.
- 5) **Edit Mode:** Select Edit as the Mode to see the zone filled in. Click and drag the markers to adjust the zone shape and size. Please refer to the image below.



- 6) **Category: Label the zone.** This feature is optional and is used for informational purposes only.
- 7) **Move Map to:** Enter the new address to change the location on the map and select "Go!"
- 8) **Save Zone:** Saves the newly created zone.
- 9) Select 'Back to Zone List'" to return to the zone list after creating the new zone.

—IMPORTANT SENTINEL ADVANTAGE—

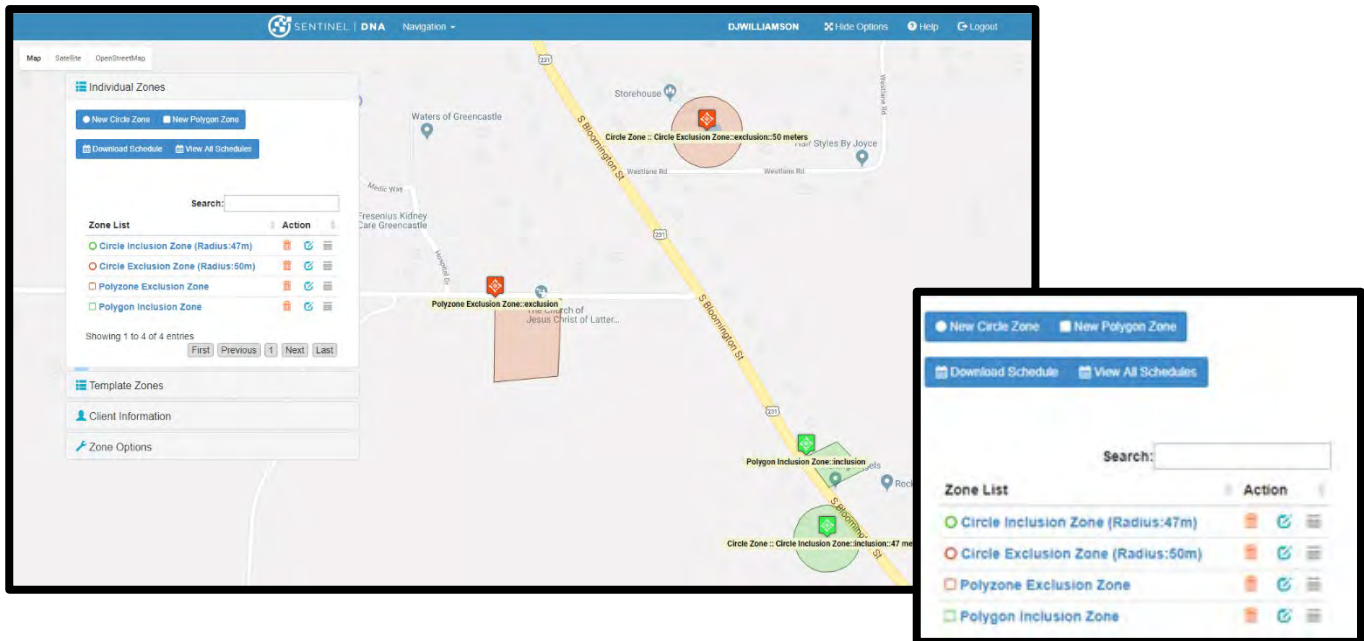
DNA allows for the use of **Individual Zones** that create pre-set zone placements for an individual program participant. To simplify the creation and use of zones, DNA places an icon in every zone (individual zone or template zone) to indicate the type of zone shown on a map.

When an agency officer views a participant's tracking data from the mapping screen, the zones, along with the detailed information about each zone, are displayed including the name of the zone, the zone type (inclusion or exclusion), and the zone radius if it is a circle zone. Polygon zones are also available to better track an offender in urban locations and are also displayed within the participant's tracking data from the mapping screen. This allows authorized users to access meaningful location information while reviewing participant zone activity without moving away from the mapping screen.

As shown in the images below, DNA visually differentiates zones with color-coding (Inclusion Zones = **GREEN**; Exclusion Zones = **RED**). From the Zones screen, **circle zones are represented in the list by a circle and polygon zones are represented in the list by a square**.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



—IMPORTANT SENTINEL ADVANTAGE—

Sentinel's DNA utilizes Google Maps® which provides automatic updates to the system always delivering the latest maps and upgrades. DNA tracks its own points and overlays the points on the most recent Google Maps® available at the time of tracking.

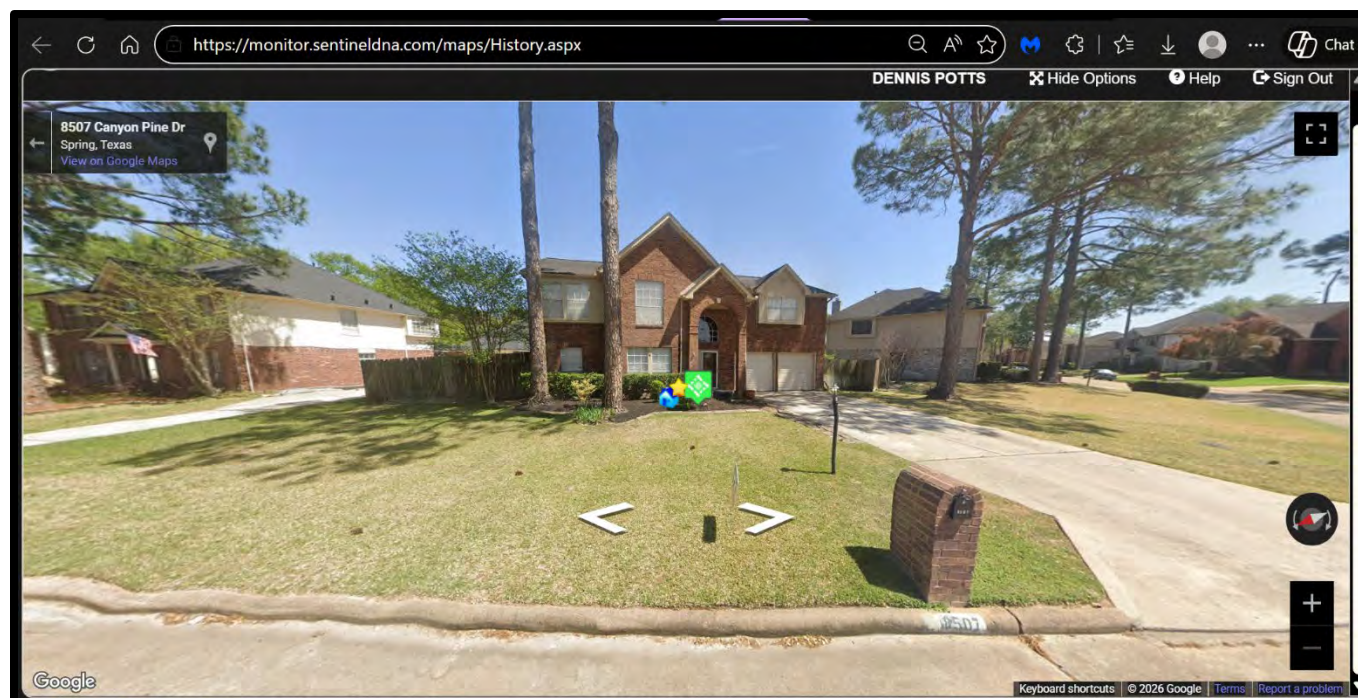
DNA uses Google Maps to provide authorized users with three (3) levels of mapping options: satellite images, street maps and hybrid maps (satellite imagery overlaid with street maps). There are also multiple distinct views including traditional, bird's eye, and street view. These interactive maps contain easily recognizable images at the global level as well as down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking data on the map. With the click of the mouse button, DNA allows authorized users to "drill down" from a high-level view of a participant's overall tracking down to his/her tracking movements at a specific location.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



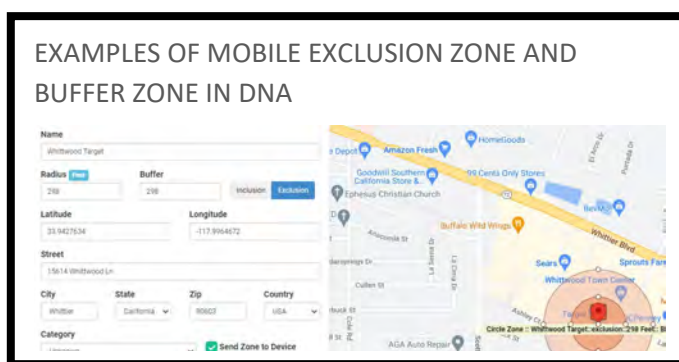
DNA STREET VIEW USING GOOGLE® MAPS



—IMPORTANT SENTINEL ADVANTAGE—

In addition to the ability to create individual **Inclusion and Exclusion zones in the shapes of circles, rectangles, and arbitrarily shaped polygons, as well as being able to have zones within zones**, Sentinel's DNA web-based system will also allow the agency to create / establish **advanced warning parameters by including buffer zones around exclusion zones** to alert individuals of an upcoming potential violation of the zone. DNA also allows agencies to utilize mobile exclusion zones in addition to stationary exclusion zones.

GPS Buffer Zones: Buffer zones provide an extra layer of notification around exclusion zone borders and **enhance notifications to allow for a 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. This places 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 buffer and exclusion zone area.



Mobile Exclusion Zones (MEZ): Mobile Exclusion Zones (MEZ) allow agencies to track if a participant on GPS monitoring comes near another specific individual anywhere, they may be in the community. Often used for victim notification applications and in domestic violence cases, the victim has a zone which is created around their smartphone while the perpetrator/participant wears an OM500 GPS tracking device.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Sentinel incorporates the use of the MEZ format through our **Advocate™, Victim Notification and Tracking Application**, which enables the configuration of the Mobile Exclusion Zone (MEZ) around the victim's smartphone and utilizes the victim's smartphone to acquire and report GPS data to our DNA monitoring system. Advanced GPS monitoring technology tracks the location of both the offender and the victim. If the OM500 device comes within an agency specified distance of the victim's smartphone, the victim receives notification on their smartphone of the Mobile Exclusion Zone breach giving her/him necessary information to help initiate her/his safety plan. Additionally, law enforcement may be contacted at the discretion of the Agency.

The Sentinel offender/victim tracking solution gives officers the ability to continuously monitor an offender's proximity to their victims. The locations of the offender and the victim are recorded as historical data giving officers insight into how much time an offender is spending in the vicinity of a victim. The size of the Mobile Exclusion Zone is determined by court order or the agency and may range from hundreds of feet to hundreds of miles. The Mobile Exclusion Zone also incorporates the use of a Buffer Zone in order to create an extra layer of notification and enhance the agency's tracking capabilities when utilizing the Advocate Victim Notification and Tracking Application.

—IMPORTANT SENTINEL ADVANTAGE—

Victim/participant separation is achieved using exclusion and buffer zones that create notifications on participant entry. However, use of these zones may impose impractical restrictions on participant travel; e.g., blocking a participant's ability to maintain employment, attend treatment or court sessions. With permission and when circumstances warrant, thoughtful application of **Neutral Zones** allows monitoring agencies to schedule limited **Travel Paths** into or through zones; i.e., exclusion zones, inclusion zones, and buffer zones.

The main function of neutral zones and travel paths is to prevent zone alerts when a device is within a designated "neutral zone" or "travel path" area during the allowed schedule time. When the neutral zone / travel path is active, buffer and exclusion zone alerts will be suppressed, and enter/exit events are only recorded for the neutral zone unless the participant deviates from the neutral zone or travel path. Please note that if a device enters an area covered by an overlapping buffer or exclusion zone outside of the neutral zone schedule or travel path, alerts for those zones will be triggered as usual. The following scenario illustrates how neutral zones and travel paths function in practice.



Travel Path Overlapping Large Exclusion Zone: The issue presented is that a client's work location requires the client to pass through a buffer/exclusion zone; as shown in the image below, the client must travel down a main highway to reach their place of employment, however a large exclusion zone covers the highway. The solution is to **create a neutral zone schedule as a travel path** to allow the participant to travel through the zone at pre-set specific times when the neutral zone takes priority, as depicted in the following screen shot.



—IMPORTANT SENTINEL ADVANTAGES—

- + **Entering Travel Path Outside Schedule:** If a Neutral Zone has a schedule (e.g., 7 am to 8 am) and the device enters the travel zone after the schedule ends (e.g., after 8 am), alerts will be raised for the Exclusion zone.
- + **Deviating from Neutral travel Path:** If a client travels through a Neutral Zone travel path overlapping Buffer and Exclusion zones during the allowed schedule time but deviates from the Neutral path, alerts will be raised as expected for the first point plotted outside the Travel Path and within the exclusion zone.

SHADOWATCH (OPTIONAL)

Agency staff can easily create zones around a physical address. Zones can be created utilizing a Polygon, State/County, or Circle. Polygon Zones can be customized by creating the exact shape needed. Circle Zones can be customized to create the exact size of the zone needed. State/County Zones are automatically created around the borders of the desired States or Counties. Zones can be created specifically for an individual participant or shared between multiple participants.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack|McAndrew, Tom (Shadowtrack)

Zone Name

Massachusetts Probation

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

Street

1 Ashburton Place

Unit

Room 405

City

Boston

State

MA

Zip Code

02108

Country

United States

Find Location

Center

(42.35990412639689, -71.0623588005265)

Radius (ft)

374.06

MAC Address

Save

Cancel

shadowtrack

PROVIDING SOLUTIONS IN CORRECTIONS USING ADVANCED TECHNOLOGY

Shadowtrack|McAndrew, Tom (Shadowtrack)

If you want to edit the coordinates of an existing polygon, click it to enable edit mode.

Zone Name

Massachusetts

Default Location

Yes ☒ No ☐

Exclusion

Yes ☒ No ☐

Beacon

Yes ☒ No ☐

State-wide

Massachusetts

County

MAC Address

Save

Cancel



6. Describe your customizable reporting. How does the reporting work with court requests and chain of custody requirements for legal purposes.

SENTINEL RESPONSE

CUSTOMIZABLE REPORTING FOR OM500

SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

COURT REQUESTS AND CHAIN OF CUSTODY REQUIREMENTS FOR LEGAL PURPOSES FOR OM500

Sentinel will immediately contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Entity's Data.

Sentinel utilizes a Corporate Custodian of Records in our organization to be the gatekeeper of official subpoenas and Departmental requests for data as it relates to Sentinel's role in the monitoring, supervision, alert notification, and conformance of the delivery of contractually agreed upon service levels.

Sentinel can provide records from our DNA system as well as from our Engineering and Quality Assurance Departments in a variety of formats which can be sent via certified mail and/or electronically. Sentinel will include all data requested by the agency.

We understand the required testimony obligations, and Sentinel will provide a subject matter expert to appear in court to discuss equipment, monitoring services, etc., if required. We are fully prepared to provide qualified personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports under oath in a court of law. Upon request of the court and/or in response to a subpoena, Sentinel will provide expert court testimony, either in person or in writing, through witnesses qualified to defend the integrity of our systems and services on behalf of the agency. We also can provide testimony via secure virtual web-based sessions, as needed, which became essential during the COVID pandemic.

We are able to submit the monitoring documentation as supporting evidence when describing the program participant's activities while being monitored. All court testimony is supported by our Custodian of Records who will attest to the validity and accuracy of all monitoring documentation.

When Sentinel receives a records request directly from the court, we produce responsive records in accordance with legal and chain-of-custody requirements. These records are typically accompanied by a **Business Records Affidavit** to establish authenticity and admissibility without the need for live testimony.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The affidavit affirms that:

1. The attached business records were made at or near the time of the events described by, or from information transmitted by, a person with knowledge of those events.
2. The records are kept in the course of Sentinel's regularly conducted business activities.
3. Creating and maintaining these records is a regular practice of Sentinel.

CHAIN OF CUSTODY FOR OM500

To preserve chain of custody for legal purposes:

- + Records are extracted directly from the system of record by authorized personnel.
- + The data is maintained in its original format, without alteration, and any exports are documented.
- + Access, handling, and transmission of records are controlled and traceable to ensure integrity and authenticity from creation through production .

CUSTOMIZABLE REPORTING FOR SHADOWWATCH (OPTIONAL)

The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the Participant Entity's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing participant access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

Shadowtrack has a wide array of report options ranging from violation reports to inventory control that can be downloaded, printed, and/or exported in various formats. From within the monitoring platform, supervising personnel can easily review/download/print/export the activity of a single participant or generate additional reports specific to the Participating Entity's needs. Many of the reports already available were requested by other customers. Reports are available via various formats including PDF, Excel, etc.

- + Case Load at a Glance
- + Alcohol Monitoring Tests
- + Missed Test / Check in
- + Automated and Ad Hoc Reports
- + Event History
- + Multi-point client enrollment
- + Client deactivation
- + Analytics

CHAIN OF CUSTODY FOR SHADOWTRACK SHADOWWATCH (OPTIONAL)

The Shadowtrack System is SOC II Certified and preserves full chain-of-custody integrity through secure data handling, system controls, and documented quality-assurance measures.

Key elements include:

- + **Secure, Centralized Data Storage.** All alcohol readings, breath test results, test location points, participant demographic details, and photos are stored in the Cloud within a secure, audit-controlled environment. Shadowtrack's activity is cloud-based, and access to the case management system or any



of the raw data requires two-factor passcode identification and authorization along with other security measures.

- + **Permanent Event Logs.** Every monitoring event is captured with a permanent timestamp and cannot be altered, ensuring complete traceability from device generation through reporting
- + **Quality Control and Assurance.** A formal quality-control program ensures documentation accuracy and compliance with evidentiary standards across the country.
- + **Subpoena Compliance.** When subpoenaed, Shadowtrack immediately notifies Participating Entities and assigns personnel directly responsible for the monitoring information to provide requested information ensuring proper representation of chain-of-custody handling and data interpretation.

Shadowtrack ensures all data remains secure and legally defensible throughout the contract life cycle.

7. Describe how often the device collects a point and reports the location within a set time frame.

SENTINEL RESPONSE

OM500

The OM500 can be remotely programmed to a variety of different transmission rate plans, as intensive as tracking at one (1) point per minute and reporting the information every minute as well as a less intense plan that tracks one (1) point per minute and reports the information every ten (10) minutes. Other reporting intervals are also available based on agency preferences. **It is important to note that regardless of the reporting interval setting, alerts such as Tamperers and Exclusion Zone Violations are always reported immediately.**

Through the DNA monitoring system, our proposed solution provides the flexibility an agency needs for tracking these rate plans or levels of supervision each participant receives to meet individual monitoring needs. This level is defined by the type of monitoring assigned in the participant's equipment profile. The equipment profile not only defines the monitoring intensity but also allows the agency to change the level based on a participant's current monitoring status. It is important to know that at any time the rate plan can be changed to collect points more/less frequently and to report the information at differing intervals. It is also important to note that, **when in an Exclusion Zone or while in Pursuit Mode, the OM500 device increases its acquisition timers and collects location information every fifteen (15) seconds then reports the data to the web-based information system every thirty (30) seconds.** The most common profiles are identified below but may be customized to meet agency requirements as desired.

MONITORING PROFILE	MODE OF OPERATION	DESCRIPTION OF RISK
Active Monitoring	Acquires a GPS point every one (1) minute and transmits data every ten (10) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every five (5) minutes. Tamperers and Zone Violations (Zones on Board) are immediately transmitted.	Riskiest participants requiring a very high level of supervision
Hybrid Monitoring	Acquires a GPS point every one (1) minute and transmits data every thirty (30) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamperers and Zone Violations (Zones on Board) are immediately transmitted.	Moderate participants requiring intensive supervision

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Passive Monitoring	Acquires a GPS point every one (1) minute and transmits data every sixty (60) minutes and includes an Impaired Location (Wi-Fi/cell tracking) every fifteen (15) minutes. Tamper and Zone Violations (Zones on Board) are immediately transmitted.	Lower risk participants requiring only standard supervision

—IMPORTANT SENTINEL ADVANTAGE—

Industry Leading Triple Tracking Capability via GPS, Wi-Fi and Cellular Tracking Location Points. In impaired areas where GPS cannot locate the device, the device automatically collects the IDs and signal strengths of visible Wi-Fi networks and cell towers for always-on, high precision secondary tracking. This allows for a significantly more robust device as it offers multiple tracking options that are included at no additional cost.

SHADOWATCH (OPTIONAL)

The ShadoWatch device can be set to various tracking intervals including 1-minute location intervals and 5-minute location intervals based upon the Participating Entity's desired preference and location data will be reported to the ShadowtrackONE monitoring platform. The ShadoWatch is equipped with multiple location technologies. Tracking data is achieved through the ability of the device to obtain its location through GPS Satellite data and Wi-Fi data, as well as Location Based Services (LBS). The primary mode of tracking is obtained by GPS, with secondary location data being obtained if the devices are in an area of limited or poor satellite coverage (i.e. indoor locations, etc.). Each location point contains the latitude/longitude coordinates if tracking data is obtained through satellite signals, the MAC address if location is obtained through secondary Wi-Fi locations, or lastly by cellular triangulation (LBS) if neither GPS or Wi-Fi signals are detected. The system automatically translates and geocodes this data into a precise address where the participant is located.

8. Describe your Customer Service, including at least the following:
 - a. Hours of operation
 - b. Order procedures (how long to respond to order, delivery time frame). Delivery time after receipt of order? Describe online ordering procedures.
 - c. Product request response time (what is kept on hand at office vs ordering products) – inventory on hand

SENTINEL RESPONSE

Sentinel owns, staffs, and operates both its Primary Monitoring Center and Secondary Monitoring Center. Sentinel owns both the primary National Monitoring Center located at Sentinel's Norco, California, corporate office) and a geographically redundant secondary back-up monitoring center in Atlanta, Georgia. Sentinel's monitoring centers are staffed with trained personnel 24/7/365 and at no time are monitoring services outsourced or subcontracted.

HOURS OF OPERATION

Our monitoring center is staffed 24 hours a day, seven (7) days a week with a supervisor always on duty and live operators cross-trained to support our suite of supervision services and products. This staffing allows Sentinel field staff and agency staff to call and speak with one of our monitoring experts at all times of the day or night. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

Sentinel also provides access to designated help desk staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. This specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

—IMPORTANT SENTINEL ADVANTAGE—

Multiple Warehouse Distribution Centers

To aid our customers, Sentinel a Primary Warehouse located at 1220 North Simon Circle, Unit C, Anaheim, California as well as a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia. With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers. Both locations are open five (5) days a week during normal business hours from 08:00-17:00 daily.

ORDER PROCEDURES

Sentinel's Help Desk is the point of contact for the ordering of new equipment and the Return Material Authorization (RMA) process. New and return orders are received by the Help Desk via a SentinelDNA monitoring system submission, email, phone call or fax from the customer. Return Material Authorization (RMA) requests submitted to Sentinel are received by the designated Help Desk representative who is responsible for ensuring the order is properly processed and the customer confirmation email is delivered.

In accordance with Sentinel's Ordering Process, all orders received by 12:30 p.m. (Local Time) are prioritized, processed, and shipped on the day the order is received. Orders received after 12:30 p.m. (Local Time) are processed and scheduled for shipment the next business day.

In accordance with Sentinel's shipping process, orders are prioritized and processed based on the expected Arrival Date at the customer's location. Sentinel staff add new orders received to the Open Orders Report. Once the order is ready to be processed, staff will print and review the Order Details Report for adequacy and prepare the order utilizing one of the shipping methods below. The staff will then change the order status to 'completed' and remove the order from the Open Orders Report once the order has been shipped.

Sentinel's standard shipping method is Ground shipping at no cost to the Participating Entity. For Entities that desire express shipping Sentinel also offers the following shipping methods.

+ Ground Shipping (1-5 business days)	+ 2 nd Day Early AM
+ Express Saver	+ Standard Overnight
+ 3 Day Shipping	+ Priority Overnight
+ 2 nd Day Air	

REQUEST RESPONSE TIME

Sentinel maintains a core inventory of high-demand electronic monitoring equipment at its U.S. distribution centers to support rapid order fulfillment. Requests for items maintained in inventory are typically processed and shipped within one (1) business day of request receipt. Inventory levels are actively managed based on historical usage and forecasted demand to ensure availability and consistent service levels. New devices are received



weekly at our warehouse locations and at all times Sentinel maintains available inventory in both the Anaheim and Alpharetta warehouses to ensure timely delivery of customer orders. The volume of weekly deliveries may be increased or decreased based on forecasted needs to ensure warehouse inventory remains available at all times.

Additionally, Sentinel provides equipment for our customers that is stored at the customer's location. This "Shelf Stock" is available to address the day-to-day inventory needs of the program and to allow for ebbs and flows of program size without the need to order/return devices. The amount of Shelf Stock a customer chooses to utilize is determined by program operations, participant enrollments and duration of time on the program. Entities typically carry approximately 10%-15% of shelf stock at any given time.

9. How do you comply with local and state regulations (what type of research do you conduct when working with a new entity?)

SENTINEL RESPONSE

Sentinel strives to remain current and advocate support of legislative initiatives and regulatory initiatives in favor of, never in conflict with, Participating Entity initiatives. Sentinel has been providing electronic monitoring services since 1993 and today operates in more than 40+ states. Since inception, Sentinel has monitored social and political changes that have shaped the criminal justice system and the resulting alternative to incarceration programs where we provide services. Each state and local jurisdiction is subject to laws and regulations that Sentinel complies with both operationally and contractually. With the assistance of Sheppard Mullins, a leading law firm based in California, Sentinel reviews existing and pending legislation and accurately modifies contract documents, participating agreements, amendments, and adjusts operational procedures to remain compliant with local, state and federal regulations. When appropriate, Sentinel supplements our team with attorneys from local jurisdictions to track and monitor legislation that is potentially impactful to the electronic monitoring industry and/or interests of our Entity partners.

When Sentinel receives an inquiry about our products and services or when we approach a government entity and they express a desire to learn about our continuum of products and services, our sales team will research the procurement requirements for that agency as well as research local and/or state statutes that stipulate the use of Cooperative Purchasing Programs. Sentinel has found this to be very effective in our consultative approach as once the agency determines they want to utilize Sentinel products and services, we share with them details on the researched statute and on the cost, time, and convenience, the NASPO ValuePoint Cooperative Purchasing Program and the Sentinel Electronic Monitoring Services Contract provides.

Sentinel understands and has experienced the regulatory nuances that must be addressed and complied with both contractually and operationally from county to county and state to state. Examples of Sentinel's regulatory understanding and compliance include the July 1, 2021, California Assembly Bill #1869 that removed various fees for the cost of administering home detention programs and continuous electronic monitoring. Sentinel tracked, communicated with our government customers, and modified all our impacted contracts to ensure continued compliance. Additionally, we modified our on-site equipment installation and collections services to comply with these new laws. Another example of staying abreast with regulatory requirements includes legislation in the state of South Carolina S.367/H.3532 for bond release and requiring electronic monitoring providers to be approved by the South Carolina Law Enforcement Division (SLED). Sentinel has met the SLED Standards and is Certified in the State of South Carolina. Our local staff have completed the required background checks, drug testing and training in accordance with Sentinel and SLED standards. Our record keeping policies are performed in accordance with standards and the required SLED reporting is provided as required. As a SLED certified provider, Sentinel has facilitated information sharing by granting access to our monitoring system to law enforcement agencies.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



All of Sentinel's products and services comply with applicable laws. All our products are FCC approved, registered, and certified as required by the cellular networks on which our devices communicate.

Sentinel does not distribute, sell, or otherwise share any information captured during the participant's electronic monitoring period and all records and data remain the sole property of the supervising entity. Moreover, Sentinel complies with all subpoena requests and has an internal Standard Operating Procedure that dictates the steps to be taken to secure evidentiary material and communicate with the legal stakeholders when a subpoena has been served.

Our attorneys along with our senior management team, which have more than 200 years of combined experience in the electronic monitoring industry, will continue to monitor legislative and regulatory changes to ensure ongoing compliance with all applicable laws. Further all future products are developed and certified by the FCC and cellular providers as required to comply with all local, state and federal regulations.

10. Describe the on-boarding process for new Participating Entities.

SENTINEL RESPONSE

SENTINEL ON-BOARDING PROCESS

Sentinel's customer on-boarding is a simplified and strategic process of guiding new Participating Entities through introduction of Sentinel's field operations team and the initial planning session that includes discussions on agency setup, review of training curriculum, and discussions on the transition of the products and services to help them achieve their first "win" and value realization with the emphasis aiming to build confidence, improve efficiency, and establish long-term, productive relationships.

Following mutual authorization of the Participating Addendum, Sentinel works with the Participating Entity to finalize an On-Boarding Work Plan and Timeline that includes all known contacts, tasks, deliverables, milestones, and duration estimates for each task and resource loading for the duration of the project. We understand the importance of open and fully transparent operations in the provision of public safety solutions and believe it is essential to the effective operation of any electronic monitoring program. We meet with Participating Entity personnel weekly during the initial implementation stages to review progress, performance, and to identify and resolve any programmatic challenges.

After mobilization, Sentinel continues to meet with the Participating Entity as necessary monthly or quarterly depending on the needs of each Participating Entity. We continue to provide all written reports to the Participating Entity as needed to operate an efficient and effective program including participant activity reports for each program participant and monthly summary reports. In addition, the Sentinel Regional Account Manager continues to always be available through telephone and/or email communications to address concerns or resolve issues with the program.

We work closely with the Participating Entity to ensure all needs, including implementation timeline expectations, are met during implementation and transition. We are highly flexible in our capability for mobilization and adjust our plans and staffing requirements as needed per the decisions mutually agreed in the Initial Project Briefing and Information Session. The following is an example of the elements involved in Sentinel's On-Boarding Process:

On-Boarding Work Plan Milestone	Week 1	Week 2	Week 3	Week 4	Monthly Beginning at Program Start
Initial Project Briefing and Information Session: • Introduction of Sentinel Resource Contacts					

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



(Sales, Account Manager, Monitoring Center, Help Desk, Accounting/Billing)					
• Networking with other Sentinel Participating Entities for sharing Programmatic Policies and Best Practices					
• Confirmation/Schedule of Initial Order(s), Training and Transition					
• Agency Notification Profiling, what assistance, if any does the entity need with transferring existing program participants demographic data into Sentinel's Monitoring Application					
Pre-Production Project Evaluation and Analysis					
Design, Development and Testing					
On-site Program Staff Installation and Training					
Equipment Delivery					
Department Training					
Participant Enrollment & Equipment Transition					
Operation and Maintenance					
Assessment of Initial Order Fulfilment					
Ongoing Contract Monitoring and Reporting					

11. Describe the on-boarding process for new Clients. Include any installation information that may apply.

SENTINEL RESPONSE

PARTICIPANT ORIENTATION PROCEDURES

At the first meeting with staff, program clients are provided a full program Orientation. During this Orientation, the rules and regulations of the program are explained, and the client is required to sign the Participant Agreement, which has been customized to meet the needs of the program. Upon completion of the review of the Participant Agreement and based on the activities that the client is allowed to conduct, daily curfew schedules are established clearly detailing when the client can leave their residence for permitted activities.

Staff only allow those activities that are Participating Entity-approved and were established prior to program implementation. In order to verify their whereabouts while away from the residence, the client is instructed what documentation is required for them to provide at all subsequent compliance appointments. The other tasks at the Orientation include:

- + **Schedule Review** | All daily curfew settings will be reviewed for accuracy and to verify compliance with Participating Entity-approved activities.
- + **Residential Confirmation** | The client will be required to provide proof of his/her residential location. Staff ask for proof of rent payment, monthly home payment note, or official correspondence that verify the client's place of residence.
- + **Contact Verification** | The client will be asked to provide alternate contact methods. In addition to their personal telephone or cellular numbers, staff attempt to obtain other contact options including contact



information for a spouse, friend, or other relative. These additional contact numbers are important when staff are researching an alarm or similar event. All these contact numbers are entered into the proprietary case management system.

- + **Fee Setting** | For those program clients requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule set up with the client.
- + **Next Appointment Setting** | Based on the required reporting schedule of the client, the next face-to-face meeting (Compliance Appointment) will be set at this time. The client will be provided with the appointment information as well as any required documentation that is needed to accompany them in order to ensure compliance.
- + **Question and Answer Support** | If there are any program related questions, the staff member will answer these for the client. If the client ever requests unusual changes such as a modification to their permitted activities, staff will immediately contact the designated Participating Entity personnel to inquire if the change(s) can be approved. Staff will NOT make any changes to the permitted activities or residential status without the prior approval of the designated Participating Entity personnel.

All this information is entered into the client's personal case file in the proprietary case management system, with copies of the statements also kept in the client's physical file at the program office. Participating Entity personnel can have secure access into the case management system to view all case manager-generated reports and notices at any time.

EQUIPMENT INSTALLATION PROCEDURES

Prior to the completion of the Enrollment process (further described below), staff install the required monitoring hardware on the client. As required, staff will perform all necessary steps for "installing" equipment, including enrollment, capturing initial enrollment images for visual compliance-related equipment, etc. The customary equipment installation procedures include:

- + **Preparation of Equipment** | Based on the level of monitoring required, staff will prepare the appropriate equipment type for installation. All equipment is tested by the Sentinel National Warehouse for performance prior to shipment to local field offices.
- + **Data Entry** | Staff will enter the required client information in the monitoring system in order to activate the necessary monitoring or tracking equipment for said client.
- + **Sizing** | If ankle-worn equipment is required for the client, staff will size and fit the ankle-worn device on the client. This is accomplished by adjusting the hypoallergenic ankle strap down to an appropriate size and attaching it to the security holding backplate, which keeps the ankle strap in place. As a higher security option, the OM500 GPS device is available with a metal-reinforced strap that greatly reduces the chance of unauthorized removal by the clients.
- + **Installation** | The designated device is secured onto the assembled strap and backplate assembly.
- + **Activation** | The device is activated, and a "good hook-up" is confirmed in the monitoring system. This confirmation is done at the field office to ensure that the client's device is operating as required prior to their departure.
- + **Equipment Guide** | For situations where the client is issued multiple pieces of monitoring equipment, e.g., radio frequency (RF) monitoring and alcohol testing equipment, the staff member will instruct the client how to install the equipment at their residence, in addition to providing them with an instructional flyer illustrating the simple in-home install process if needed.

The Installation process is complete at this time and the monitoring and/or tracking equipment will begin to report all activity and alert information as required. The installation of an ankle device is completed in less than five minutes.



ENROLLMENT PROCEDURES

As the Orientation is being completed, staff create and submit an **Enrollment Notice** to the designated Participating Entity personnel thereby confirming the enrollment of the selected client has been completed. This enrollment notice contains all pertinent client and case information so that the Participating Entity knows all details of the supervision guidelines.

On the Enrollment screen, staff can enter all equipment information, i.e. field monitoring device number, transmitter number, etc. This information is used to properly control Sentinel's internal inventory system for both hardware and accounting purposes. It also allows personnel to quickly ascertain the unit number that a client has been assigned in order to generate monitoring center activity reports.

12. Provide screenshots showing the functionality and user experience of the web-based platform and the mobile platform.

SENTINEL RESPONSE

SCREEN IMAGES OF DNA MONITORING SYSTEM SHOWING FUNCTIONALITY AND EASE OF USE

DNA provides a single point of entry for Participating Entity personnel to set up and access information related to program participants. DNA allows the technologies proposed herein to communicate on a web-based platform enabling users to easily and efficiently manage their program caseloads. Agency officers will have the ability to view comprehensive participant data, including creation of and access to individual participant profiles, current and historical monitoring data, violation status, and notification settings whether the participant is active, inactive, or pre-enrolled. DNA also includes the ability to upload a photo for participant identification.

Once an authorized user is logged in to DNA, the system navigates to the home screen which displays caseload data on a **Dashboard**. The Dashboard is designed to allow for a fast review of the status of all program participants through easy-to-understand alert icons and battery indicators. The Dashboard provides authorized agency staff with the flexibility to view all or selected subsets of their entire caseload in near real time. The following information is displayed on the Dashboard as a quick snapshot:

+ Violation Status	+ Equipment Status
+ Participant Name	+ Compliance Status
+ Pre-Enrollments	+ GPS Battery Level
+ GPS Location (world icon)	+ Notification Profile
+ Client ID (System generated)	+ Officer
+ Type of Monitoring (RF, GPS)	

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Located to the right of the **SentinelDNA™** logo at the top of the Home Screen/Dashboard are three horizontal lines. Clicking on these lines allows authorized users to access the Navigation menu which opens to the left of the Dashboard display.

The screenshot shows the SentinelDNA dashboard interface. At the top, there is a blue header with the SentinelDNA logo and a 'Sign Out' button. Below the header, a navigation menu is visible on the left side, containing links for Dashboard, Enrollment, Reports, Operators, Management, and Administration. The main area of the dashboard displays a table of participants. Each row represents a participant and includes columns for Name, OID, Type, Equipment, Compliance, Battery, Profile, and Officer. The table is sorted by Name, and the first few rows show participants with IDs like 101228, 121123, and 131313. A red arrow points to the three horizontal lines next to the SentinelDNA logo, indicating the location of the navigation menu toggle.

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 each participant. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, location information (via mapping), equipment status, current battery status, as well as zones and daily curfew schedules.

This screenshot shows another view of the SentinelDNA dashboard. The interface is similar to the previous one, but the table of participants is sorted by Name. The first few rows show participants with names like Anderson, Chad Verizon Test, BART, Amy, and BART, DJ. The table includes columns for Name, OID, Type, Equipment, Compliance, Battery, Profile, and Officer. The dashboard also features a search bar at the top right and a navigation menu on the left. The overall layout is clean and organized, designed for easy navigation and data viewing.

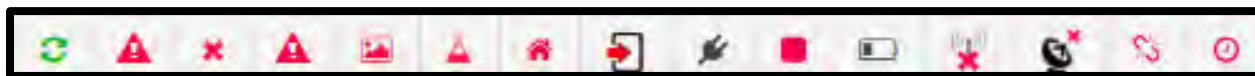
Authorized users can refine the information displayed by clicking any of the dashboard headings (Name, OID, Type, Equipment, etc.) to re-sort the information based on that parameter. This allows agency staff to quickly view participants by type of monitoring, by alert, or even by battery percentage. In addition to sorting the information by column, icon buttons (shown below) displayed at the top right of the Dashboard allow the user to filter participants

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



based upon the selected criteria such as displaying all participants who have a Tamper alert by selecting the Tamper icon.



Below the sort icons, DNA has a local search option (shown below) to make it easy to refine the dashboard display to specific participants using a first or last name. This allows the user to quickly locate a participant without scrolling through the full caseload list.

🔍

From the Dashboard, clicking on the participant's name provides a quick snapshot containing the following information:

1. Client Personal Info including Client Photo
2. Client Equipment Info
3. Agency
4. Icons to navigate to the Client Info page, Schedule page, Equipment Page, Location history page, Zones page, Notification Profile Page, client Activity page, etc.
5. Client Activity containing the last 25 events
6. Compliance Status
7. Equipment Status
8. GPS Battery Status
9. The last known GPS Location

The Client Personal Info (1), Client Equipment Info (2), and Agency (3) boxes at the top of the screen are static and provided at the top of all pop-up screens. Please see the screen image below with corresponding numbers.

● GPS, Only
✕

1

OID	ID895167
Name	GPS, Only
Home Ph	8005896003
Work Ph	
Cell Ph	
Address	201 Technology Dr, Irvine, CA-92618

2

Type	GPS3
IMEI	3E432E76
Receiver ID	
Transmitter ID	DT042963
GPS Phone	18012597127
Timezone	PST

3

Name	Software Development Group
Officer	QA Dev
Cell	
Office	
Email	
Timezone	PDT

Clear All Alarms
Client Info
Schedule
Equipment
Location
Zones
GPS Actions
Profile
Activity
Refresh
Add Note
4

5

6

Event	Received Time
User Entered Note	1/17/2017 9:36:08 AM
test by QA2	
User Entered Note	1/17/2017 9:35:49 AM
Client - ID895167 was deleted on 2017-01-17 by QA Dev @ Jan 17 2017 9:35AM	
User Entered Note	1/13/2017 5:23:42 PM
Client temporary schedule update for 2017-01-20: NEW Friday (Wrap - Wrap)	

7

8

9

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Below we have provided examples of the Client Activity and Equipment Status screens.

DNA CLIENT ACTIVITY SCREEN

Client Personal Info		Client Equipment Info		Agency	
OID	ID6719830	Type	GPS3	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT000000	Officer	Training Department
Name	HELM Tester, AT&T OM500	IMEI	10000809	Cell Phone	714-726-1114
Home Ph	(800) 589-5003	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csuazn@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Simon Cir Anaheim, CA 92805			Support Staff	None
TimeZone	PST			TimeZone	PST

Event	Event Time	Received Time
Work Failed To Enter Inclusion Zone	10/21/2025 8:30:10 AM	10/21/2025 8:30:09 AM
Work Late To Enter Inclusion Zone	10/21/2025 8:20:24 AM	10/21/2025 8:20:23 AM
Notification sent to: monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
Notification sent to: monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
KMTR Tamper - GPS	10/21/2025 8:02:20 AM	10/21/2025 8:02:47 AM
Backplate Tamper	10/21/2025 8:02:20 AM	10/21/2025 8:02:46 AM

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. **This provides all the important participant information on one screen.**

DNA CLIENT EQUIPMENT STATUS SCREEN

Client Personal Info		Client Equipment Info		Agency	
OID	ID6719830	Type	GPS3	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT000000	Officer	Training Department
Name	HELM Tester, AT&T OM500	IMEI	10000809	Cell Phone	714-726-1114
Home Ph	(800) 589-5003	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csuazn@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Simon Cir Anaheim, CA 92805			Support Staff	None
TimeZone	PST			TimeZone	PST

Status	Event Time	Action
HOME	Since 3/14/2025 8:03:46 AM	
GPS(Strap) Tamper	10/20/2025 6:05:29 PM	Clear
BackPlate Tamper	10/20/2025 6:05:29 PM	Clear
Potential Shielding		
Potential Slippage		
MEZ Enter		

As illustrated in the Equipment Status screen image above, the client's current location is shown on the map to the lower left along with the current status of the device including any tampers along with the date and time of occurrence. Officers can quickly view if there is a device issue without wasting time.

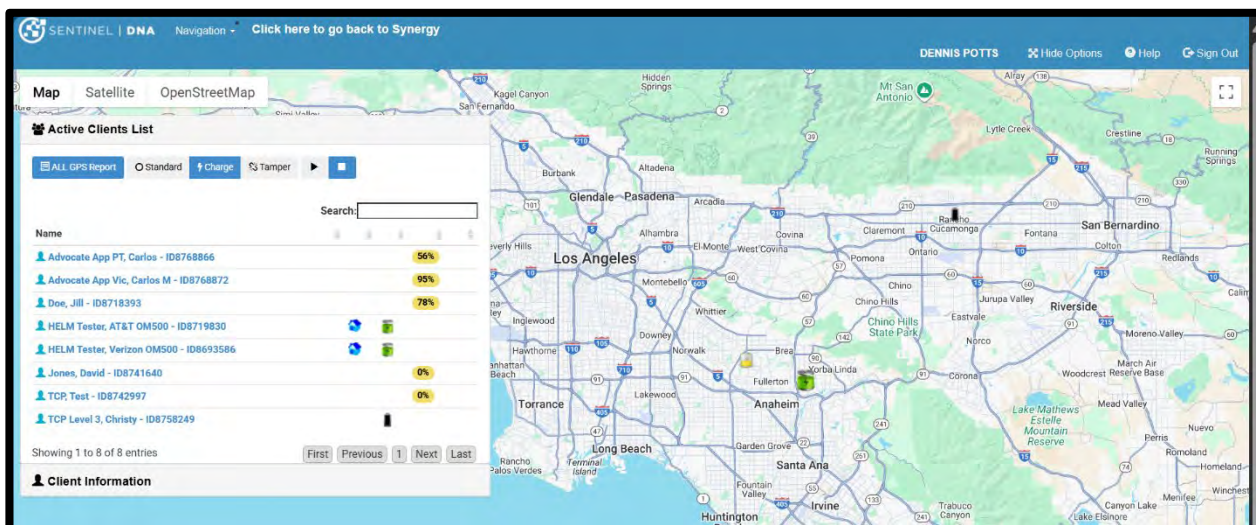
As illustrated below, DNA also gives officers the ability to view the battery status of every device assigned to their entire caseload from a single screen. DNA provides pop-up style notification windows to display caseload details with visual indicators for each participant on a map to the right of the caseload window.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

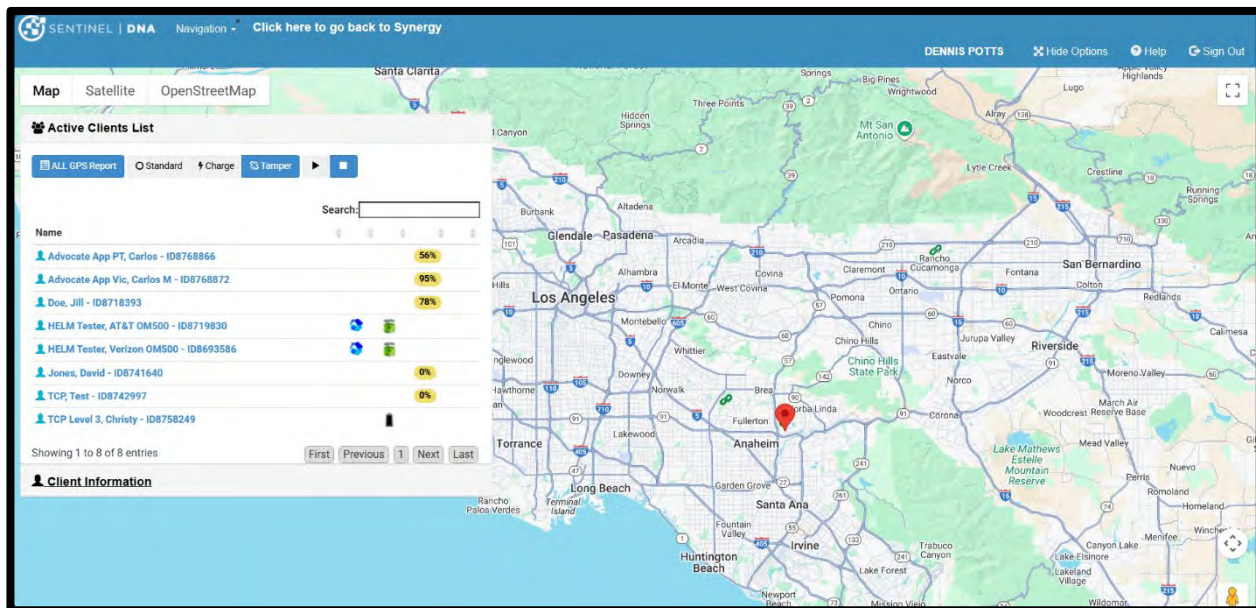


DNA CHARGE / BATTERY STATUS SCREEN



DNA provides the same detail regarding the tamper status of all devices assigned to an officer's caseload. As illustrated below, visual indicators help officers to quickly locate and identify potential issues and/or violations in their caseload. Devices in tamper are indicated with a red icon on the screen below.

DNA TAMPER STATUS SCREEN



MAPPING TOOLS

Sentinel's DNA utilizes Google Maps® which provides automatic updates to the system always delivering the latest maps and upgrades. DNA tracks its own points and overlays the points on the most recent Google Maps® available at the time of 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). There are also multiple distinct views including traditional, bird's eye, and street view. These interactive maps contain easily recognizable

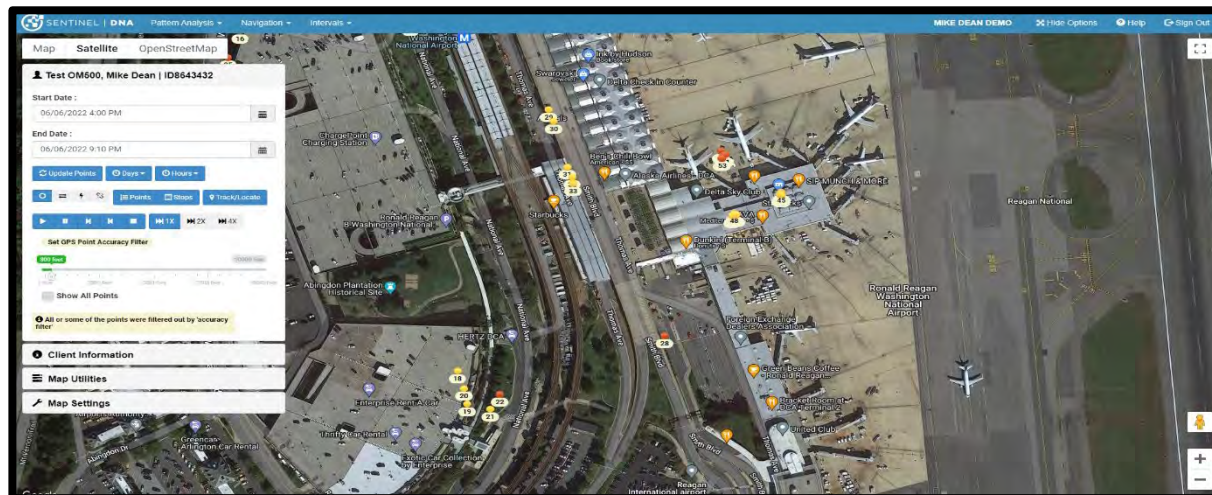
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

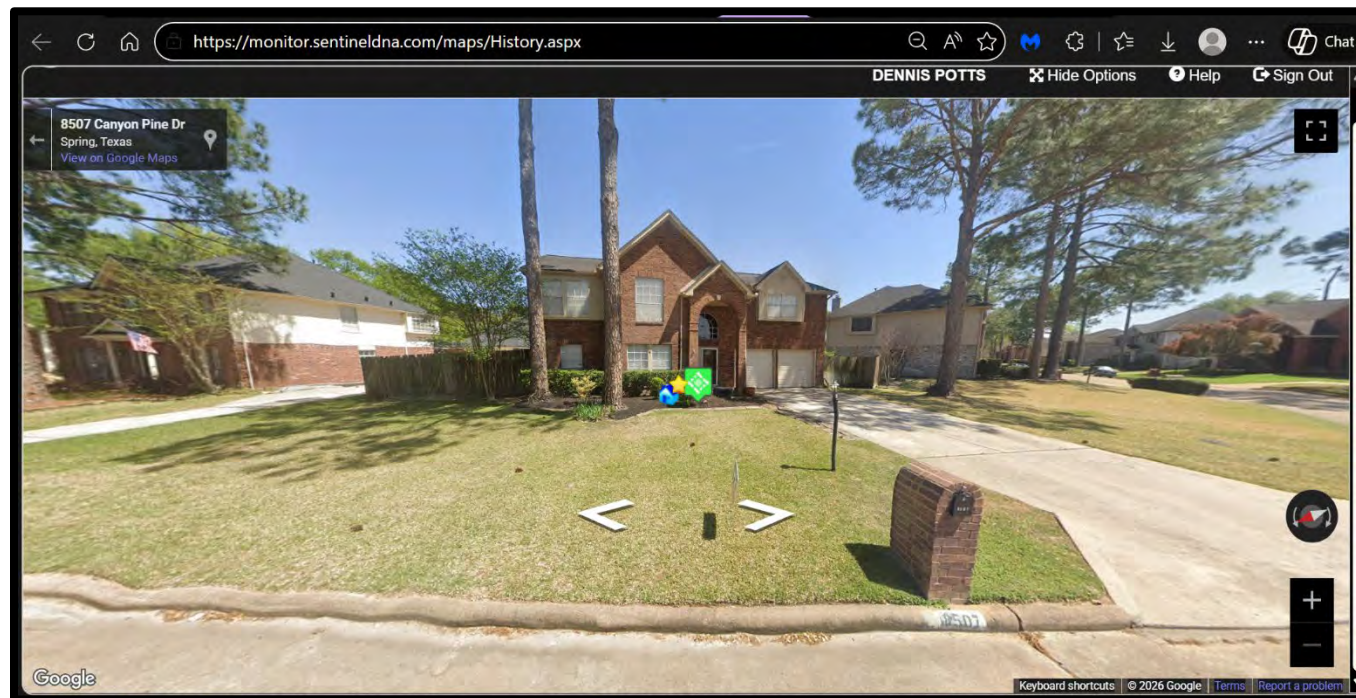


images at the global level as well as down to street level. DNA enables authorized users to easily zoom in and out when viewing tracking data on the map. With the click of the mouse button, DNA allows authorized users to “drill down” from a high-level view of a participant’s overall tracking down to his/her tracking movements at a specific location.

DNA SATELLITE VIEW USING GOOGLE® MAPS



DNA STREET VIEW USING GOOGLE® MAPS



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA offers several mapping utilities that allow authorized users to customize the mapping tools to better suit their needs. **Map Utilities** allow users to center the map around a specific address while **Map Settings** allows the user to enable or disable a variety of map features.

- + **Show client track:** Connects points during playback to illustrate the order.
- + **Show track direction:** Adds arrows to the client track to indicate participant direction.
- + **Center map while animating track:** Centers the map on each point during playback.
- + **Filter points while the client is HOME:** Hides points collected while the participant was within the HOME inclusion zone.
- + **Show Template Zones:** Place an icon on the map for each template zone assigned to the participant.
- + **Show Individual Zones:** View or hide individual zones on the map when viewing the participant's location.
- + **Stack Points:** Groups consecutive points located in the same geographical area.
- + **Show Numbered Labels:** Enables the chronologically numbered labels on the points
- + **Show GPS Accuracy:** Enables the GPS Point Accuracy Filter
- + **Show Locations Labels:** Allows to hide locations pin on the zone map view.
- + **Grid Size:** Adjust the size of the area in which the points should be grouped as one stack.
- + **Stack Min Duration:** Filters out locations where the participant was present for less than a specific time duration.

A screenshot of the "Map Settings" interface. It features a list of settings with checkboxes. The settings are: "Show client track" (checked), "Show track direction" (checked), "Center map while animating track" (checked), "Filter points while client is HOME" (unchecked), "Show Template Zones" (unchecked), "Show Individual Zones" (checked), "Stack Points" (unchecked), "Show Numbered Labels" (checked), "Show GPS Point Accuracy" (checked), and "Show Location Labels" (checked). At the bottom, there are two input fields: "Grid Size" with the value "100" and "Stack Min Duration" with the value "0".

SCHEDULING

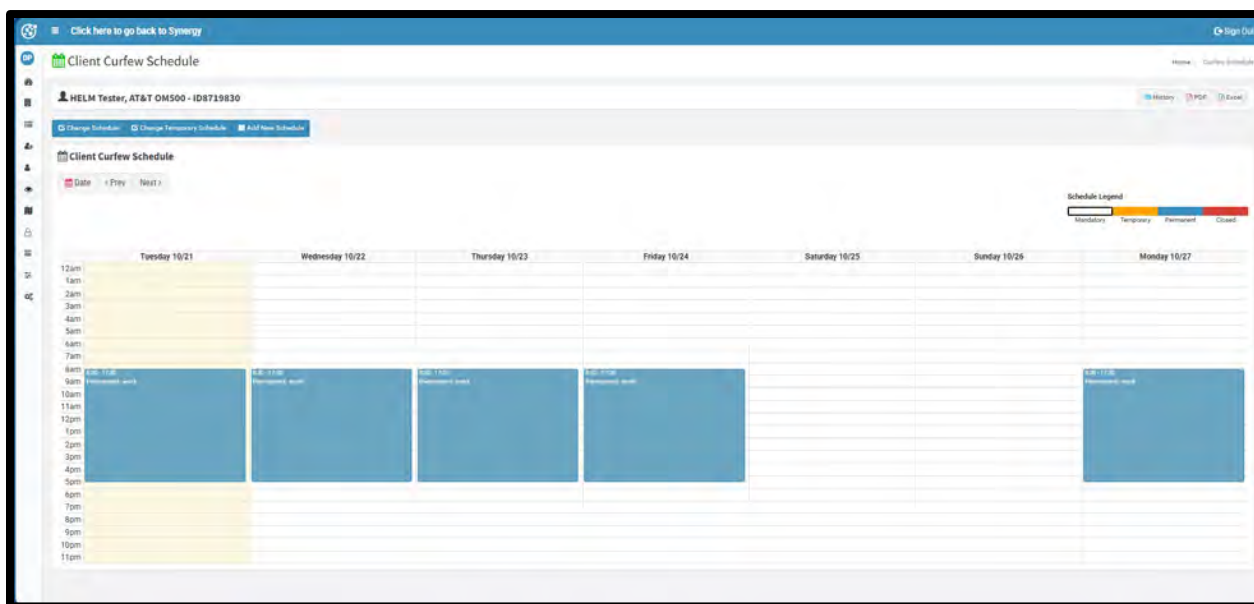
Scheduling. During program enrollments, staff enter curfew/zone schedules and/or inclusion and exclusion zone schedules for each program participant in our DNA web-based system. SentinelDNA zone schedules allow supervising entities to select specific periods when a participant is required or is not allowed to be within a geographical location (zone). All zone enter and zone clear events are triggered by points within or outside a zone. Each exit from, and entry to, the residence or zone (inclusion or exclusion) is reported by the GPS unit, and the DNA web-based system automatically compares the activity's location with the set zones. The OM500 GPS devices, coupled with our SentinelDNA web-based system, provide reliable residential monitoring eliminating the need for home monitoring units or beacons. 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 always ensures the monitoring of each program participant. **DNA also has the capability to create permanent and temporary schedules for both GPS and RF clients and to copy and paste a schedule from one day to the next.**

Request for Proposals for ELECTRONIC MONITORING

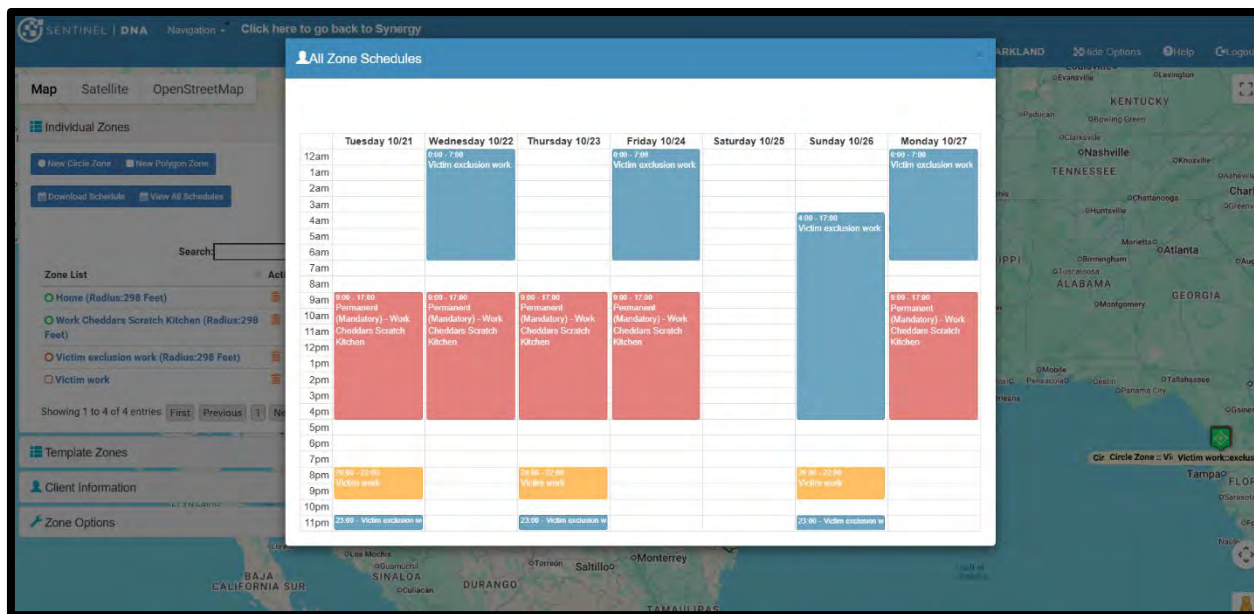
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA GPS CLIENT CURFEW SCHEDULE SCREEN IMAGE



DNA GPS CLIENT ZONE SCHEDULE SCREEN IMAGE



Schedules within DNA define specific time periods when the client is required to be home or is permitted to leave his/her home. If no schedule is assigned to the client, the default setting for each client schedule is "Closed" – meaning the client is not permitted to leave the residence.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

A screenshot of the "Client Curfew Schedule Editor" web application. The interface shows a calendar grid for a client named "DUALTRAK TESTER 1 ANTHONY - ID838820". The left sidebar has a "Copy/Paste" section with buttons for each day of the week, and a "Change Time Frame" section with radio buttons for 5, 15, and 30 minutes, and a "Full" button. The main calendar grid shows a schedule for Sunday through Saturday. On Sunday, there is a blue block from 12am to 11pm labeled "Client is allowed out all day". On Monday through Friday, there are blue blocks from 8am to 5pm labeled "Client is allowed out from 8am to 5pm". On Saturday, there is a red block from 12am to 11pm labeled "Client is required to be home all day".

ZONE CREATION

Authorized users will have access to create, edit, and delete exclusion and inclusion zones for participants being tracked via the GPS tracking device. **SentinelDNA allows for a virtually unlimited amount of exclusion and inclusion zones per participant.** For participants with challenging zones, DNA is also configured to support construction of customizable 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 monitor the movement of the individual program participants.**

Zones can be created as an individual zone, if only one participant will need to use the zone, or as a template zone that can be created and stored within the system as a library of zones if there are multiple participants who need to use the same zone. **DNA allows for the creation of template zones that can be used across a specific population of participants.** This allows agency personnel to designate certain sites across a region as exclusion zones for an entire population of multiple participants. This eliminates the need to repeatedly re-create the same zones for all the individuals identified in a specific population. This type of **template zone** set-up can be used for sex offenders and other high-risk participant populations establishing zones around schools, playgrounds, or related areas of concern.

Zone Options allows supervising entities to view or hide circle and/or polygon template zones on the map, view or hide location labels and zone pins, or re-center the map to a specific address.



Creating a New Circle Zone

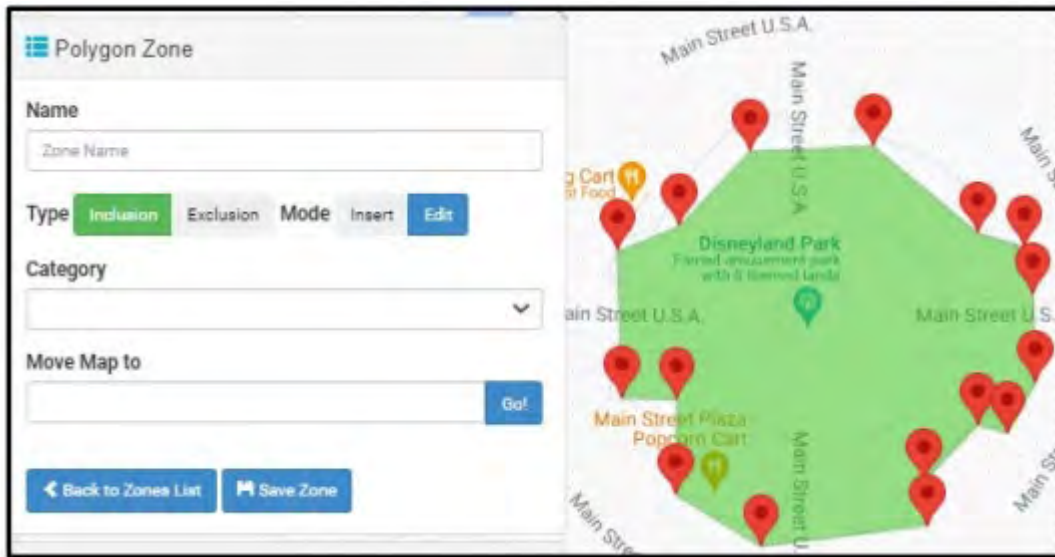
- 1) Select 'New Circle Zone'.
- 2) **Name the zone.** IMPORTANT: If creating a zone for the participant's residence, the zone must be named "Home" to associate the zone with the participant's curfew schedule. A "Home" zone should NOT have a zone schedule. Instead, the Home zone will exclusively rely on the participant's curfew schedule.
- 3) **Radius:** Select the size of the zone (measured in feet).
- 4) **Inclusion or Exclusion:** Select Inclusion if the participant is allowed to enter the zone. Select Exclusion if the participant is not allowed to enter the zone.
- 5) **Latitude and Longitude:** This will auto-populate after entering an address and selecting Move to this address.
- 6) **Street:** The circle zone will default to the home address of the participant. To change the address and move the zone to another location, enter the new address and select "Move to this address."
- 7) **Category: Label the zone.** This feature is optional and is used for informational purposes only.
- 8) Select 'Save Zone' to save the newly created zone.
- 9) Select 'Back to Zone List' to return to the zone list after creating the new zone.

A screenshot of a web form titled "Circle Zone". It contains fields for "Name" (with a placeholder "Zone Name"), "Radius" (set to 300 feet), "Buffer" (set to 0), and radio buttons for "Inclusion" (selected) and "Exclusion". There are also fields for "Latitude" (43.5978193) and "Longitude" (-116.6458923). A "Street" field contains "1290 N Hancock St". Below this are dropdown menus for "City" (Anaheim), "State" (California), "Zip" (92807), and "Country" (USA). A "Category" dropdown is also present. At the bottom, there is a "Send Zone to Device" checkbox (checked) and three buttons: "Back to Zones List", "Move to this address", and "Save Zone".

Users can manually adjust the position of the zone, click the red zone marker icon and drag the zone to the correct location.

Creating a New Polygon Zone

- 1) Select 'New Polygon Zone'.
- 2) **Name the zone.** IMPORTANT: If creating a zone for the participant's residence, the zone must be named "Home" to associate the zone with the participant's curfew schedule. A "Home" zone should NOT have a zone schedule. Instead, the Home zone will exclusively rely on the participant's curfew schedule.
- 3) **Type:** Select Inclusion if the participant is allowed to enter the zone. Select Exclusion if the participant is not allowed to enter the zone.
- 4) **Insert Mode:** Select Insert as the mode to create the outline of the zone by clicking on the map to place markers that represent the corners of the zone. A minimum of three or as many as 16 markers can be created. NOTE: After a marker has been placed, it can be repositioned by dragging it with the cursor. Double-click on a marker to remove it.
- 5) **Edit Mode:** Select Edit as the Mode to see the zone filled in. Click and drag the markers to adjust the zone shape and size. Please refer to the image below.



- 1) **Category: Label the zone.** This feature is optional and is used for informational purposes only.
- 2) **Move Map to:** Enter the new address to change the location on the map and select "Go!"
- 3) **Save Zone:** Saves the newly created zone.
- 4) Select 'Back to Zone List'" to return to the zone list after creating the new zone.

Creating a New Buffer Zone - Circle

- 1) Name the zone
- 2) Enter the zone *Radius* and *Buffer*.
- 3) Ensure *Exclusion* is selected, and that the circle zone is red.
- 4) Enter the address. After entering the address, select *Move to this address* to move the zone to its proper location.
- 5) On the *Victims* dropdown, select any victims associated with the Exclusion Zone.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Circle Zone

Name: Victim Work

Radius: 500 Feet Buffer: 500 Inclusion Exclusion

Latitude: 33.86222 Longitude: -117.8137

Street: 1290 Hancock St

City: Anaheim State: California Zip: 92807 Country: USA

Category: Send Zone to Device

Victims: (ID: [redacted])

Buttons: Back to Zones List Move to this address Save Zone

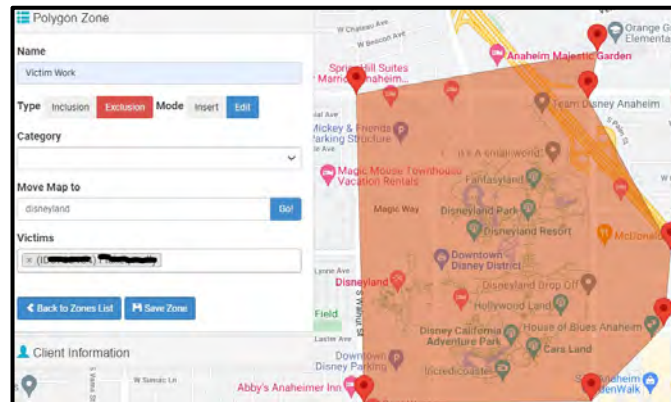
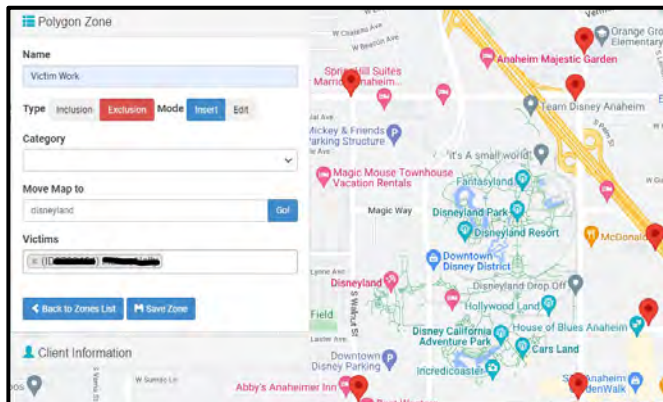
Creating a New Buffer Zone - Polygon

- 1) Name the zone
- 2) Ensure 'Exclusion' is selected and the shape of the zone is red.
- 3) Enter the address and select 'GO!' to move to the area of the address.
- 4) Select "Insert" as the Mode to create the outline of the zone by clicking on the map to place markers that represent the corners of the zone. Users may utilize as few as three or as many as 16 markers when creating a zone.
- 5) Select "Edit" as the Mode to see the zone filled in. Click and drag the markers to adjust the zone shape and size.
- 6) On the Victims drop-down select any victims associated with the Exclusion Zone.

NOTE: Creating exclusion zones as polygons, notifications of participants entering/leaving will be received based on the transmission rate of the GPS rate plan, instead of instant like circular exclusion zones.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



—IMPORTANT SENTINEL ADVANTAGE—

DNA allows for the use of **Individual Zones** that create pre-set zone placements for an individual program participant. To simplify the creation and use of zones, DNA places an icon in every zone (individual zone or template zone) to indicate the type of zone shown on a map.

POINT PATTERN ANALYSIS

Our Point Pattern Analysis (PPA) module within DNA provides automated detection/tracking of variances in participant movement patterns with both graphical and mapping views available to officers. Our Event Detection module identifies participants who were in the vicinity of an occurrence during a specific timeframe. By combining the Point Pattern Analysis and Event Detection modules within DNA, Sentinel is creating the ability to perform a search over a program's entire population database to determine if two (2) participants were within 25 meters of each other for at least one (1) minute. (Distance and time are configurable at the Participating Agency's request)

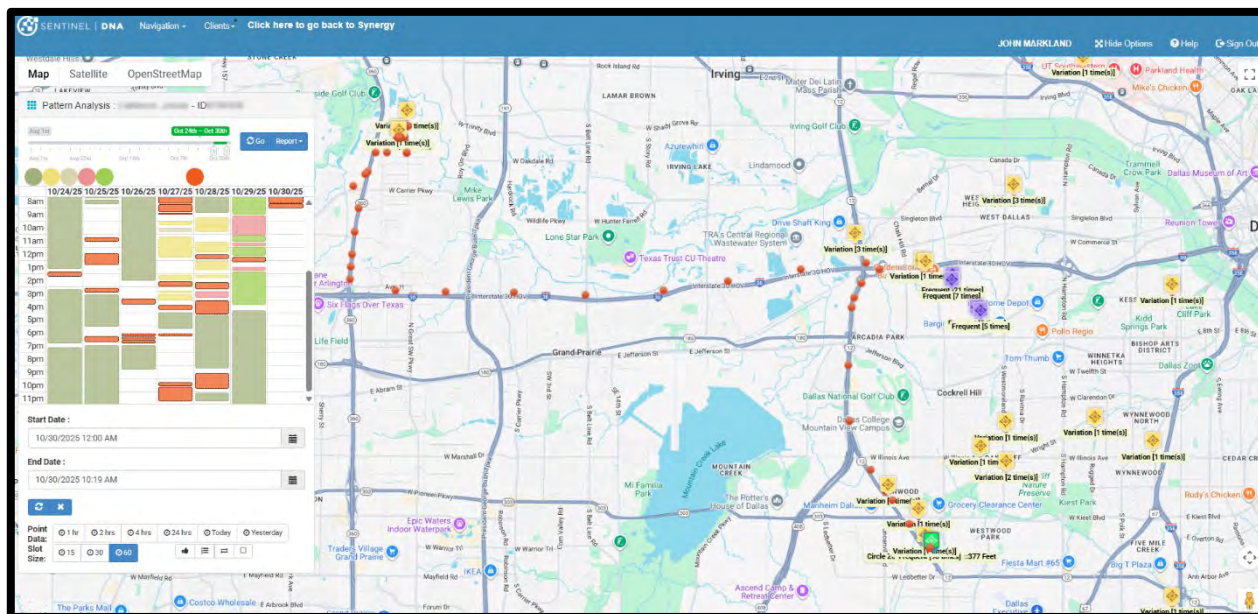
Point Pattern Analysis (PPA) is an automated analytics capability that enables users to quickly and easily identify changes in participant location/movement patterns that may be indicative of changes in behavior/compliance. To provide an agency with the most opportunities possible to create effective monitoring and in turn positive outcomes for participants, DNA includes Point Pattern Analysis (PPA) capabilities at no additional cost. This proprietary enhancement feature allows users to receive a comprehensive analysis of all their participants' routines.

Using our GPS point capture capability, our system can accurately track and display the participant's whereabouts 24/7. Although this is provided as part of the standard GPS tracking service, the advancements associated with PPA provide authorized users with a more in-depth review of a participant's tracking data. It will quickly identify "locations visited" by the participant and identify travel patterns. **PPA displays, in a detailed chart format, the periods of time when a participant was at a certain location.** The system is then 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 participant compared to variations that may be restricted locations.

Point Pattern Analysis examines locations frequented by each individual participant. 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-coding system, while locations that are new for the program participant are color coded in **RED**.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



As an example, on the map display depicted above, a user can click on the locations and the position is displayed on a Google Maps 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.

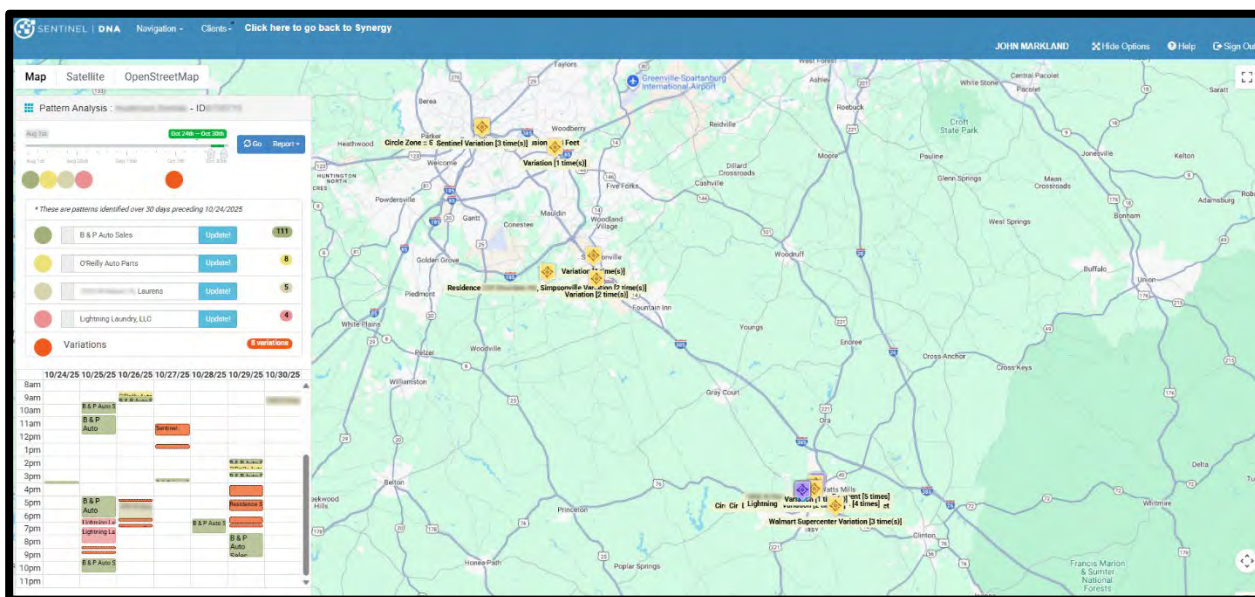
Quick and Detailed Activity History: The system can track on an ongoing basis the data points previously visited by the participant to identify and display any new locations. This allows staff to quickly see the variations in the participant's movements across the community and verify where he/she is stopping throughout the day. This PPA feature is key to assuring that the participant is not straying from his/her required schedule.

For example, if the participant is only allowed to attend work, this system should display only two locations visited, his/her residence and his/her job site. It allows for identification of travel time, which also can be used by the officers or designated personnel to confirm that the participant is not loitering during transit times between these two (2) authorized locations.

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

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



All data collected as a part of the PPA feature can be exported in a report form. The data will identify known locations based on the labels assigned to those locations as well as identify locations identified as variations using a street map view. Both known locations as well as variations are displayed within the report with the date and time of each event as shown in the image below.



Sentinel's **DNA Event Detection (Crime Scene Correlation)** feature within DNA has a mapping component that correlates crime and/or incident report data collected from local law enforcement agency stakeholders and associates the data with the tracking data of participants.

Request for Proposals for ELECTRONIC MONITORING

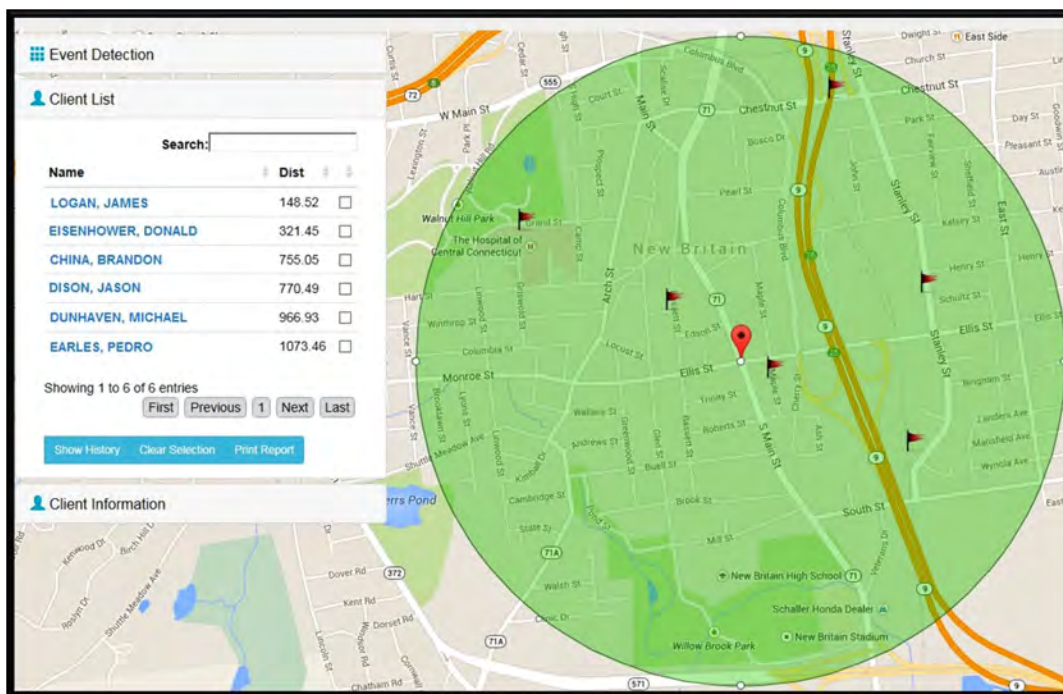
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



EVENT DETECTION

Our Event Detection mapping feature will identify participants who were in a specified vicinity of an incident address during a specific date/time range. Event Detection will simultaneously provide information for participants who are in the vicinity at the date/time of occurrence of the crime. Once the data has been entered, and the search has completed, the system will provide a Participant List and place a flag on the map for each participant in the results list and represent the location of the participant that was closest to the search address during the time frame selected.

The search results are displayed under a precise "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 address radius within the time frame selected, thereby creating a list of potential individuals for law enforcement follow up. The system also displays the participant's actual distance from the address of interest, as shown below. Furthermore, all other GPS participants can be eliminated as potential individuals as they were not in the vicinity at the date/time in question.

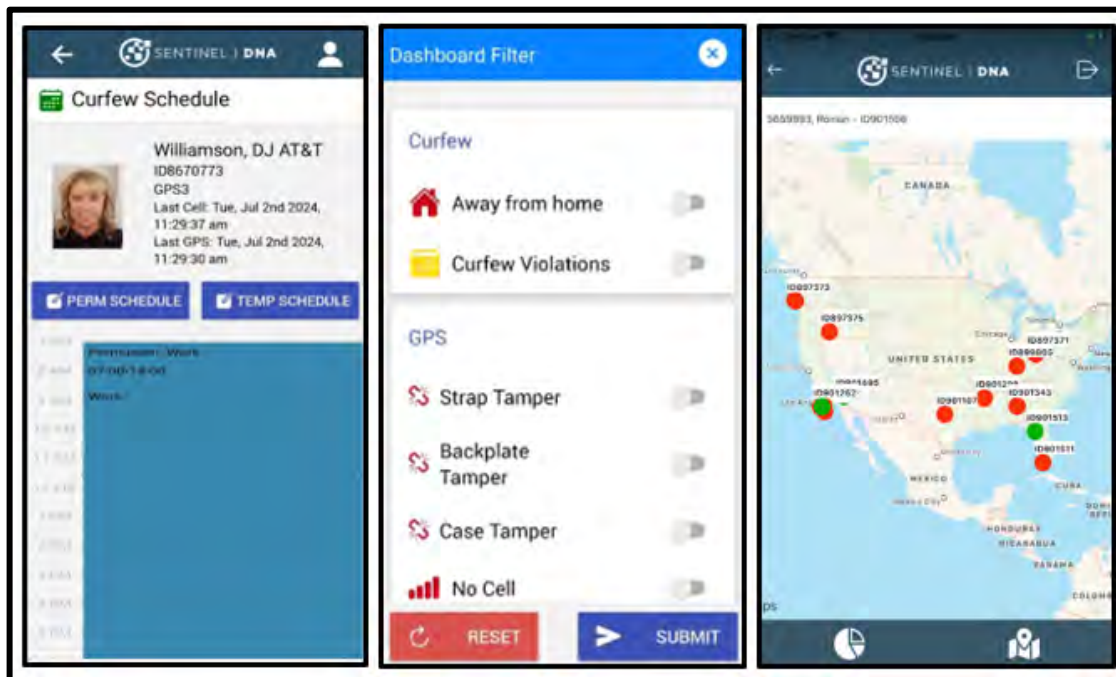
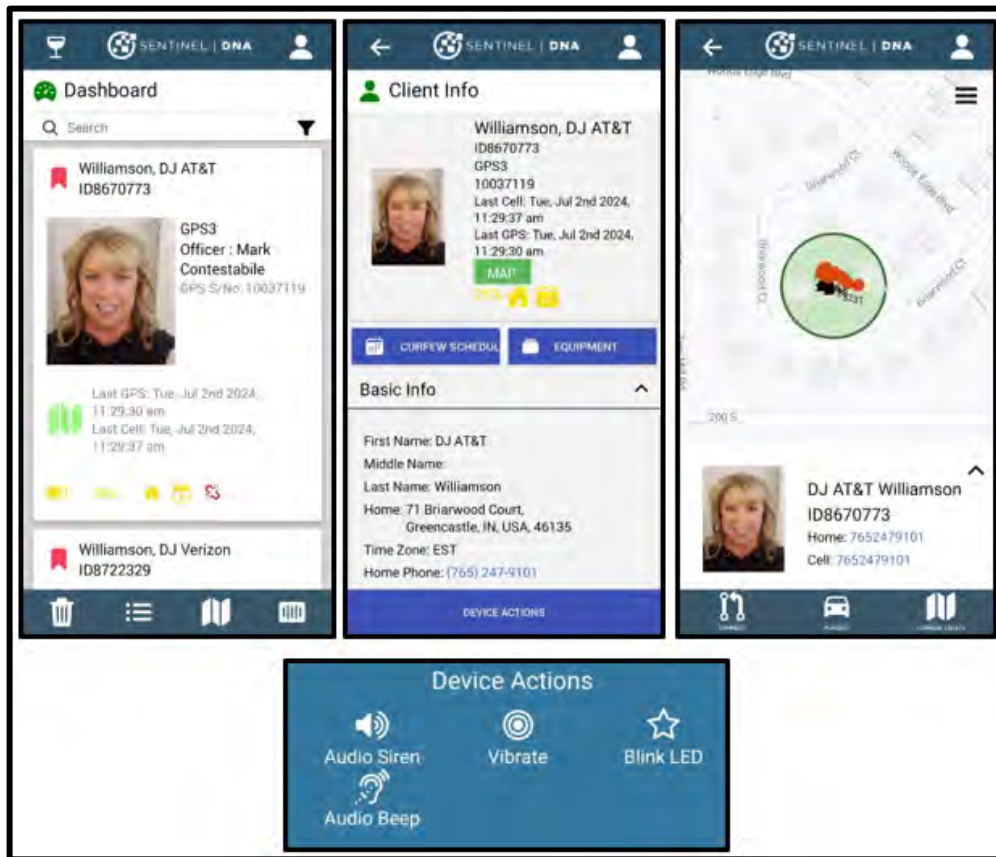


MOBILE APP SCREEN IMAGES

The **DNA Mobile Application** is designed for officer use and to streamline feature sets that are available in our full featured DNA website. The abbreviation of certain features and the addition of others in the DNA Mobile App will improve the mobile access experience of our customers using smartphones and tablets. The features of DNA Mobile App were created using valuable input from a panel of supervising officers who routinely work remotely and away from their office. DNA Mobile App facilitates remote supervision like no other and is a valuable tool in the participant supervision process.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



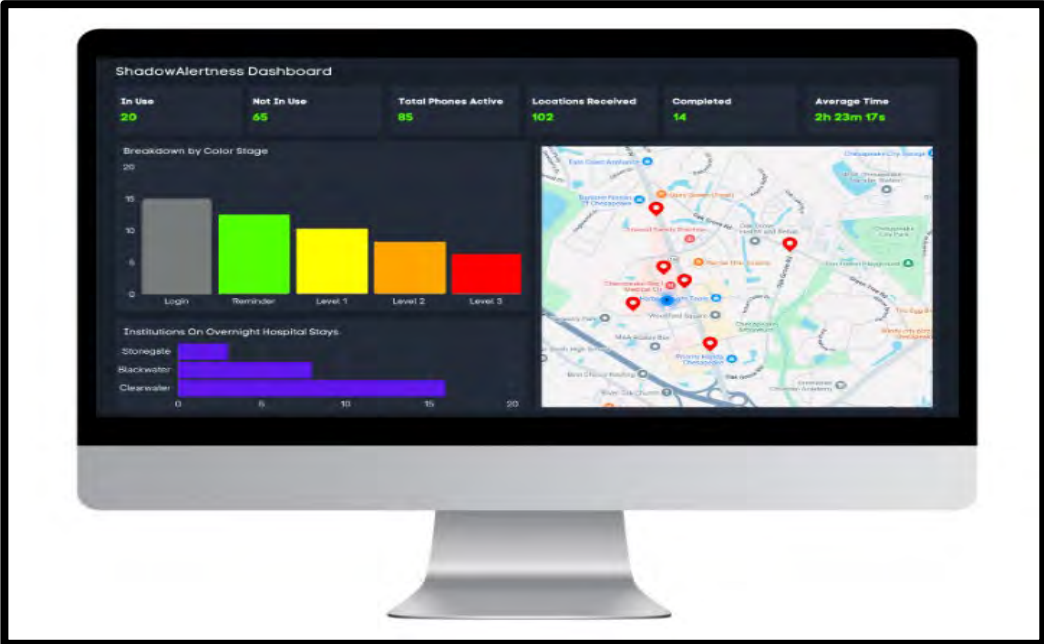
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

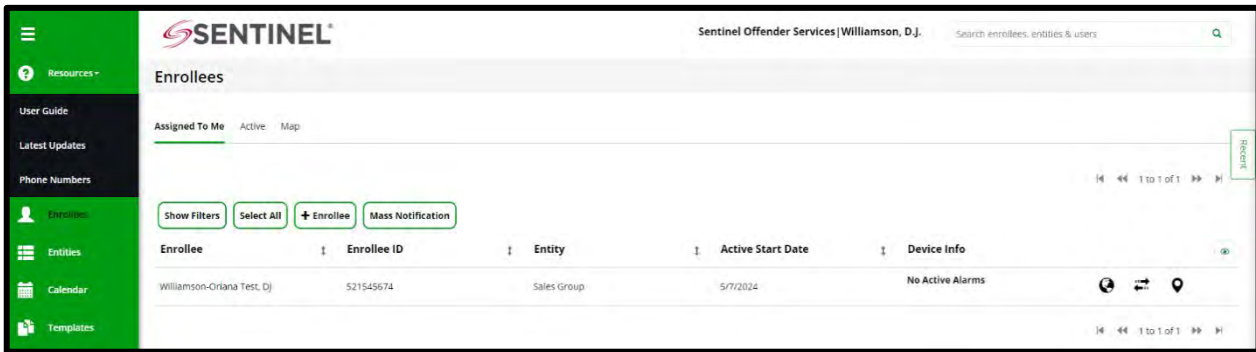


SHADOWTRACKONE MONITORING SYSTEM (OPTIONAL)

Shadowtrack is Intuitive designed to deliver real-time data tailored to the solutions being utilized, offering live insights to monitor performance, track engagement, and make informed decisions efficiently.



The Shadowtrack User's Guide is readily available for review from the left-hand menu under "Resources" and "User Guide." The "User Guide" is searchable to allow quick access to system information.



Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can easily navigate the Dashboard that displays all active participants within the agency.

The screenshot shows the ShadowTrack dashboard for Sentinel Offender Services | Williamson, D.J. The 'Enrollees' tab is selected, and a red arrow points to it. Below the tab, there are buttons for 'Show Filters', 'Select All', 'Export', '+ Enrollee', and 'Mass Notification'. The main table lists enrollees with columns for Enrollee, Enrollee ID, Entity, Assigned Officer, Active Start Date, and Watch Info. The table shows 5 enrollees, all with 'No Active Alarms'.

Enrollee	Enrollee ID	Entity	Assigned Officer	Active Start Date	Watch Info
BRAY, John (NNSCF)	521530928	SAFETRACKS GPS CANADA INC	Warren, Mike, Martin, Jeff, Alerts, Safetracks	7/12/2023	No Active Alarms
Buchanan, Quenton (P1) Paul	521530719	SAFETRACKS GPS CANADA INC	Doucette, Kristian	7/7/2023	No Active Alarms
DECOSTE, Nicholas (NNSCF)	521530674	SAFETRACKS GPS CANADA INC	Warren, Mike, Martin, Jeff, Alerts, Safetracks	7/6/2023	No Active Alarms
FRASER, Leonard (CNSCF)	521532257	SAFETRACKS GPS CANADA INC	Warren, Mike, Martin, Jeff, Alerts, Safetracks	8/16/2023	No Active Alarms
Hill, Ian	656817046	HAWAII DRUG COURT PROGRAM	Boter, Danielle, ZZZGERINGER, ZZZJACQUELYN, Custino, Jason, Gallon, Jeffrey, Kumagai, Lei, Puah, Stafford, Hubbrook, Stephen, Strickland, Troy	1/19/2022	No Active Alarms

Users can select from the Dashboard their Caseload that displays all active participants assigned to them.

The screenshot shows the ShadowTrack dashboard for Sentinel Offender Services | Williamson, D.J. The 'Assigned To Me' tab is selected, and a red arrow points to it. Below the tab, there are buttons for 'Show Filters', 'Select All', '+ Enrollee', and 'Mass Notification'. The main table lists enrollees with columns for Enrollee, Enrollee ID, Entity, Active Start Date, and Watch Info. The table shows 2 enrollees, both with 'No Active Alarms'.

Enrollee	Enrollee ID	Entity	Active Start Date	Watch Info
Test, Tony	521530958	SAFETRACKS GPS CANADA INC	7/13/2023	No Active Alarms
TEST, Dj	521530982	Bartholomew County Community Corrections	7/14/2023	No Active Alarms

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can view Participant Location History and review zone locations within the software.

SENTINEL Sentinel Offender Services | Williamson, D.J. Search employees, entities & users

Williamson-Oriana Test, DJ Sales Group Add Internal Message Request

To ensure the accurate time covers displayed, please ensure you have selected the appropriate zone on your My Account tab. If you change the time zone, please refresh the page to see your changes.

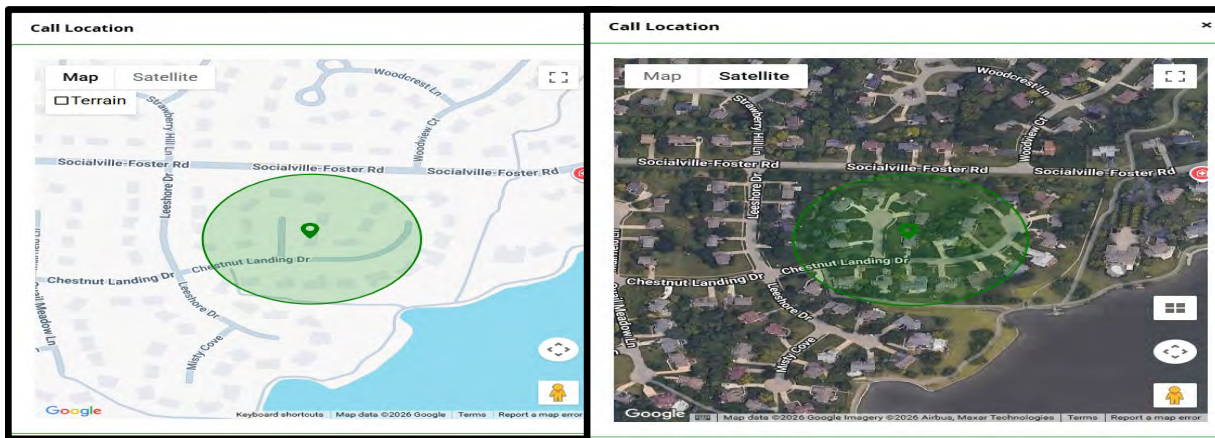
History Profile Zones Notifications Services Schedule Calendar Protocols Notes Documents Financial Check-ins

Locations Compliance Alarms

Show Filters Export

Date/Time	Status	Type	Compliance	Disposition	Location
Scheduled: 05/15/2024 11:30 AM EDT Completed: 05/15/2024 11:47 AM EDT	Complete	Interview Exceptions: 0 Questions: 4/4	Compliant	Complete Facial: Success	Inside Fence High Accuracy Location
Scheduled: 05/15/2024 10:33 AM EDT Completed: 05/15/2024 10:40 AM EDT	Complete	Video	Not Applicable	Complete	Location Verified High Accuracy Location
Scheduled: 05/15/2024 10:31 AM EDT Completed: 05/15/2024 10:32 AM EDT	Complete	Video	Not Applicable	Complete	Location Verified Medium Accuracy Location
Scheduled: 05/09/2024 01:25 PM EDT Completed: 05/09/2024 01:56 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	
Scheduled: 05/09/2024 01:00 PM EDT Completed: 05/09/2024 01:31 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	
Scheduled: 05/09/2024 12:32 PM EDT Completed: 05/09/2024 01:03 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	

Zone Images including Satellite View



Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can enter and edit Participants Profile Details

SENTINEL
Sentinel Offender Services | Williamson, D.J.
Search: enrollees, entities & users

Williamson-Oriana Test, DJ
521345678

Sales Group

Add Internal Message

History Profile Zones Notifications Services Schedule Calendar Protocols Notes Documents Financial Check-ins

Basic Information Details

First Name: DJ
Middle Name:
Last Name: Williamson-Oriana Test
Suffix:
Internal ID:
Primary ID:
Image:
Email Address:
Date of Birth:
Language: English
Time Zone: (GMT-05:00) East-Indiana/US
Address: 71 Briarwood Court, Greencastle IN, 46135, United States
Assigned Users: Williamson, D.J., Hilbert, Thomas, Simmons, Ericia, Brutto, Deana

Enrollment Phone Cases

Active: Yes
Active Start Date: 5/7/2024, 10:49 AM
Active End Date:
Enrollment Password: 16924784
Date of Voice Enrollment:
Date of Facial Enrollment: 5/7/2024, 2:21 PM
TFN Opt Out Date:

Show History Update Active Dates

Reset Enrollment Enrollment Form

Users can create and edit Participants Zones

shadowtrack
Sentinel Offender Services | Williamson, D.J.
Search: enrollees, entities & users

History Profile **Zones** Notifications Services Schedule Calendar Protocols Notes Documents Financial

Personal Shared

Map Satellite

Map

Table:

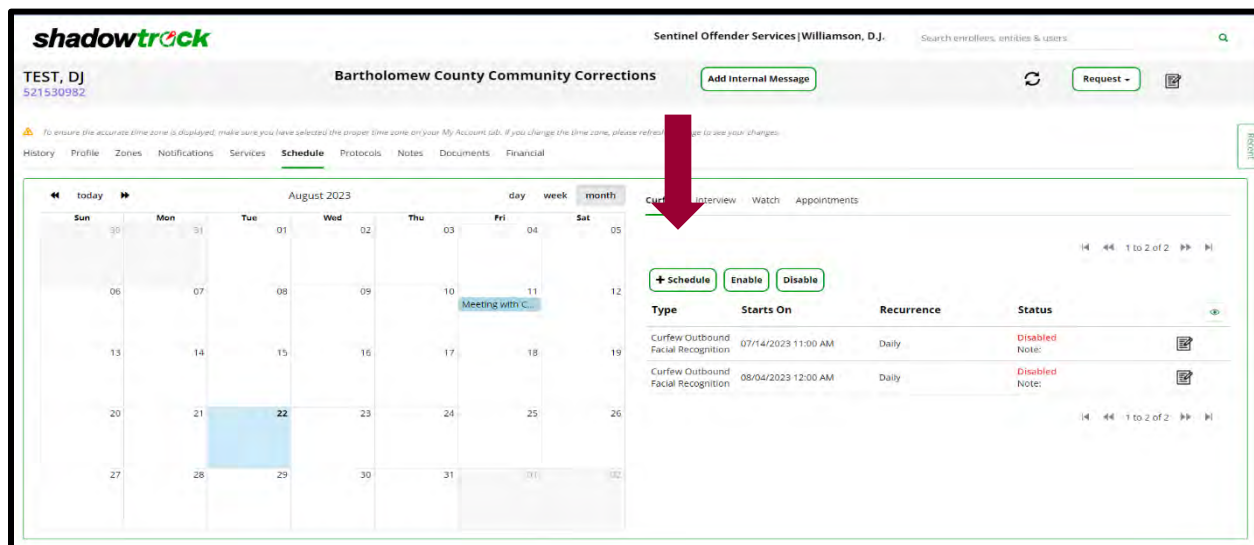
Name	Modified	Default	Exclusion
HOME	7/14/2023, 10:54 AM by Williamson, D.J.	Yes	No

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can create schedules, edit Schedules, and View in a Calendar Based Format



13. Attach the Service Level Agreement for the GPS product(s) you are proposing.

SENTINEL RESPONSE

SERVICE LEVEL AGREEMENTS

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements ("SLAs"). Please refer to the **Supporting Documentation** (page 340) of this document for Sentinel's Service Level Agreement for the GPS products we are proposing.

B. SCOPE OF WORK – CATEGORY 2: RF

- B. Scope of Work – Category 2: RF (Offerors are required to answer all questions if proposing for RF Services)

1. Describe your plan for meeting the Master Agreement Objectives identified in Attachment 02, Scope of Work.

SENTINEL RESPONSE

Below, Sentinel has provided our plan for meeting the Master Agreement Objectives for **Category 2: RF** identified in **Attachment 02, Scope of Work**.



A. RF Hardware

V. Category 2: Radio Frequency (RF) Monitoring

A. Hardware Requirements:

SENTINEL RESPONSE

Sentinel is pleased to propose the latest in radio frequency 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 continuous 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.



The RF Patrol radio frequency electronic monitoring system is comprised of a tamper-evident ankle transmitter and a home monitoring unit. The RF Patrol is designed to determine the presence or absence of a participant 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. The ankle transmitter's signal is received by the paired home monitoring unit (landline or cellular based), which reports each time the participant enters and exits from the residence. The home monitoring unit also reports any changes to the ankle transmitter's status such as a low battery or tamper alert. Both the ankle transmitter and the home monitoring unit are equipped with anti-tamper features to ensure program integrity. The RF Patrol equipment is capable of continuously signaling, receiving, storing, and disseminating data to the Sentinel monitoring center, all without any active involvement by the participant.

- All equipment and systems furnished must be standard products of the manufacturer identified, must be in proper working order and clean and free from defects of features affecting appearance, serviceability, or the safety of the client in normal intended use.

SENTINEL RESPONSE

Sentinel is the Original Equipment Manufacturer (OEM) of the proposed RF Patrol radio frequency (RF) monitoring solution, and all equipment and systems furnished will be Sentinel's standard products in working order and clean and free from defects or features affecting the appearance, serviceability, or safety of the client while in normal intended use.

- Device must use a body worn bracelet (transmitter) and a one-piece stationary home-based unit (receiver) to monitor the presence/absence of the transmitter within a specified range of the receiver and report changes in status and tampering to the Monitoring Center through standard telephone lines or by cellular telephone service.

SENTINEL RESPONSE

Sentinel is pleased to propose the latest in radio frequency 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 continuous signaling, receiving, storing, and disseminating data (through landline or cellular communications) generated by the system

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



to the Sentinel monitoring center, all without any active involvement by the participant.

The RF Patrol radio frequency electronic monitoring system is comprised of a tamper-evident ankle transmitter and a home monitoring unit. The RF Patrol is designed to determine the presence or absence of a participant 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. The ankle transmitter's signal is received by the paired home monitoring unit (landline or cellular based), which reports each time the participant enters and exits from the residence. The home monitoring unit also reports any changes to the ankle transmitter's status such as a low battery or tamper alert. Both the ankle transmitter and the home monitoring unit are equipped with anti-tamper features to ensure program integrity. The RF Patrol equipment is capable of continuously signaling, receiving, storing, and disseminating data (through landline or cellular communications) to the Sentinel monitoring center, all without any active involvement by the participant.

The RFP Patrol PTX2 (transmitter) has dual tamper resistance capabilities including both fiber-optic and case tamper. When properly installed, participants cannot remove the bracelet without damaging the case or destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot pry open, stretch, or slip off the PTX2 without detection. The RF Patrol has a 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 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 while in range. Additionally, if the PTX2 case is opened or broken light entering the internal mechanism will also generate a tamper. 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.

RF Patrol Bracelet (PTX2)



The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts to the monitoring center with date and time stamps. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU. In addition to PHMU tampers, the unit will detect and communicate all other alerts and notifications, including but not limited to PTX2 tampers, arrival and departures of the PTX2, loss and restoration of power or telephone service, and *HMU Late-To-Test*, indicative of impediments to the ability to report to the monitoring center. The RF Patrol PHMU home receiver unit is also equipped with features that generate alerts if the receiver is tampered or moved. 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 versus attempted relocation of the unit. If the unit is moved, a *Tilt In Motion* alert is generated. Should the participant attempt to open the PHMU, the unit will generate an *HMU Tamper* alert.

The RF Patrol monitoring system has a variable signal range between the PTX2 and PHMU, which is agency programmable on a per participant basis 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



The Supervising officer can quickly and easily perform a range test by accessing the Officer Control module accessible directly from the PHMU by following the following steps:

1. Turn the PHMU Menu Key to the horizontal position;
2. Select RNG (range) from the Setup Menu;
3. Select TEST from the RNG Menu;
4. The LCD screen will display the words "Testing" and a negative (-) sign to the upper left and a positive (+) sign to the right of the LCD screen;
5. The transmitter will immediately begin to blink;
6. One (1) blink from the PTX2 indicates excellent range, two (2) blinks indicate good range, three (3) blinks indicate poor signal reception, and four (4) blinks indicate no signal reception (no longer in range);
7. Installer/Officer may walk with the participant to each section of the home during the range test to confirm range;
8. Once all areas of the home have been covered, select the [<] less than symbol to end the range test and return to the main menu;
9. Once the range test ends, the PTX2 will stop blinking, and;
10. Sentinel technicians will report to the appropriate Department the range setting applied during the installation process for each participant.



RF PATROL PHMU LED DISPLAYS
FOR RANGE TESTING

- Transmitters and receivers must be field replaceable and interchangeable without the need to return them to the Contractor.

SENTINEL RESPONSE

The RF Patrol PTX2 transmitter and the RF Patrol PHMU receivers are field replaceable and interchangeable without the need to return the products to Sentinel. The transmitter and home unit are interchangeable components, enabling easy replacement of either component without replacement of the entire system.

- Installation process must be simple enough to be performed in the field by fully trained officers in less than five (5) minutes.

SENTINEL RESPONSE

With only four (4) easy to install pieces, the RF Patrol PTX2 is one of the easiest RF bracelets and straps to install in the industry. The RF Patrol bracelet is easily installed by a trained officer in less than five (5) minutes.

The RF Patrol home monitoring unit (receiver) is easily installed by a trained officer in less than five (5) minutes with simple training. The unit does not require permanent mounting. Sentinel will provide instruction and hand-out material to instruct participants in the installation, use, and care of the PHMU.

The PHMU is quick and easy for the participant to install as it does not require a skilled person to install - the participant can self-install at their residence:

- + Place PHMU on a non-metal tabletop in the center of the home, away from large metal objects or appliances
- + Connect the power cable from the PHMU to the electrical wall outlet
- + If a landline PHMU, connect the phone cord from either PHMU connector to the phone outlet on the wall - Install completed!



The RF Patrol PHMU contains internal surge protectors for power and phone lines and is installed in a central location, using a standard two-prong 110 to 120-volt alternating current power source AC power cord certified to UL standards and two (2) standard, universal RJ11C connectors that are common in participant homes (if landline unit). It is virtually impossible to connect the unit incorrectly, as officers/installers can connect either RJ11C connector to the wall phone jack or the telephone.

- The equipment must have a minimum of ~~three (3)~~ two (2) ways to communicate data to the software, such as landline, Ethernet, Wi-Fi, or cellular. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

The PHMU is available in both landline and cellular models to accommodate all participants, even those without home phone lines and uses the AT&T cellular network for communicating with Sentinel's monitoring system. The PHMU is also capable of communicating when a participant has bundled internet/phone service with VOIP, by attaching appropriate filters provided by Sentinel at the time of installation.

- The transmitter must not pose a safety hazard or unduly restrict the activities of the client. Must be lightweight, small and water-resistant.

SENTINEL RESPONSE

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 is easily, securely, and comfortably attached to the ankle of participants under normal slacks. The RF Patrol bracelet is sealed to ensure that it is waterproof and shock resistant; additionally, the unit is 100% humidity resistant. The RF Patrol PTX2 has been designed to function reliably under normal atmospheric and human environmental conditions and does not pose a safety or health threat to the wearer or unduly restrict the activities of the participant.

- The transmitter must be encased in a water-proof case that is corrosion resistant and is hypoallergenic.

SENTINEL RESPONSE

As stated above, the RF Patrol PTX2 is sealed to ensure that it is waterproof and shock resistant; additionally, the unit is 100% humidity resistant and corrosion resistant. The RF Patrol bracelet and strap are both made of hypoallergenic materials free of any external metal or alloy to avoid injury and to reduce any discomfort in wear to the participant or installer. The case is made of Acrylonitrile-Butadiene-Styrene (ABS) Plastic while the strap is made of Thermoplastic Polyurethane and neither the strap or PTX2 will corrode.

- The transmitter must be designed to prevent tracing or duplication of its signal.

SENTINEL RESPONSE

The RF Patrol PTX2 (transmitter) signal is not the same coding scheme or radio frequency used by any commercial or consumer available product. To prevent interference, tracing or duplication of the radio frequency signal, the RF Patrol PTX2 signal has a 24-bit data string with numerous unique combinations. This design prohibits duplicates or interference from other RF signals commonly found in homes. RF transmissions are the



most reliable, sophisticated, and highly encrypted in the industry. The RF Patrol bracelet uses numerous, unique **encrypted radio transmission** combinations including a constantly changing pulse rate that is unique for each active bracelet, making it virtually impossible to predict or duplicate using 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.

- The Contractor must provide either multi-length or sizeable transmitter straps with replacements provided at no additional cost to the Agency.

SENTINEL RESPONSE

Sentinel provides varying length straps for the RF Patrol PTX2 bracelet designed to fit virtually any ankle size with replacements provided at no additional cost to the Agency.

- The transmitter must be easily installed on the client with minimal training and experience. Contractor must specify the tools required and procedures to install the transmitter. The Contractor must supply the tools and equipment necessary to install the transmitters and replace the transmitter straps, at no additional cost.

SENTINEL RESPONSE

As stated above, with only four (4) easy to install pieces, the RF Patrol PTX2 is one of the easiest RF bracelets and straps to install in the industry. The RF Patrol bracelet is easily installed by a trained officer in less than five (5) minutes. The images below depict the stages and tools for PTX2 strap installation. Sentinel will supply the tools and equipment necessary to install the RF Patrol transmitters and replace the straps at no additional cost.



PTX STRAP INSTALLATION



The RF Patrol PHMU will only accept and process radio signals from the unique signal of the same participant's bracelet that has been electronically paired to by the officer. Each bracelet is interchangeable with any Personal Home Monitoring Unit as the PHMU is officer programmable to match. Thus any bracelet can easily be replaced without the need for the officer to go to the participant's home or come in contact with the PHMU. To prepare the PHMU for installation:

- + Ensure that an active and valid OPID or PMD is present prior to beginning the installation process.
- + Insert the PHMU Menu Key into the back of the PHMU and turn clockwise to the horizontal position, as shown to the right.
- + Plug the PHMU Power Adaptor into both the outlet and the PHMU. The LCD screen will illuminate and display the PHMU serial number and **Setup Menu** while the **GREEN LED** confirms a power connection.
- + Select **ENRL** from the **Setup Menu**. The Enroll Menu will appear.
- + Select **ADD** from the Enroll Menu and place the PTX2 face down on the groove on top of the PHMU. This will activate/turn the PTX on. The PHMU will begin to find any active PTX2s within range and display their serial numbers on the LCD.



NOTE: The PTX can also be activated using the supplied Key Fob. Place the bottom surface of the Key Fob in direct contact with the face of the PTX, press the top left button, and then select **ADD** from the **Enroll Menu**.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Following activation, the PTX2 LED will flash red every 8-10 seconds for 30 minutes while the Band is open or until installation is complete.

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

SENTINEL RESPONSE

Neither the RF Patrol transmitter, receiver, straps, fasteners nor clips, etc. used to install the transmitter are available to the general public.

- At least seven (7) days prior to battery failure, the transmitter must send a low battery message to the receiver and to the Monitoring Center.

SENTINEL RESPONSE

The RF Patrol PTX2 (transmitter) will emit a low battery signal to the PHMU receiver. Under normal circumstances the PTX2 will communicate a low-battery message to the receiver and reports it to Sentinel's monitoring system ten (10) days prior to depletion.

- The transmitter battery must have a minimum of one (1) year active life and a three (3) year shelf life.

SENTINEL RESPONSE

The RF Patrol PTX2 is powered by a lithium thionyl-chloride, 3.6V, 750 milliamp hours (mAh) battery pack that is designed for a continuous operating life of 24 months, proactively replaced by Sentinel at an 18-month interval and has a four (4) year shelf life.



- The transmitter must feature multiple levels of tamper detection capable of detecting disassembly of the transmitter case and/or cutting or circumventing of the transmitter strap.

SENTINEL RESPONSE

The RFP Patrol PTX2 (transmitter) has dual tamper resistance capabilities including both fiber-optic and case tamper. When properly installed, participants cannot remove the bracelet without damaging the case or destroying the strap and setting off the primary tamper circuits. Properly installed, participants cannot pry open, stretch, or slip off the PTX2 without detection. The RF Patrol has a 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 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 while in range. Additionally, if the PTX2 case is opened or broken light entering the internal mechanism will also generate a tamper. 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.

- The transmitter must be capable of storing and/or recording a tamper event that occurs out-of-range of the receiver when the transmitter returns within range of either. The tamper attempt must be communicated along with a time/date stamp.

SENTINEL RESPONSE

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 when in range of the PHMU receiver. The bracelet records and reports each tamper as a separate event alerting the agency of a participant's tamper status when the PTX2 returns back into range of the PHMU. The PHMU will report all events, including tamper attempts, with date and time stamp when the transmitter returns within range of the PHMU receiver

- Base station must be easily attached to client's phone line, Ethernet, Wi-Fi, or cellular connection. If client does not have a landline, list available options to provide wireless reporting. The total cost for RF service via landline and wireless is to be listed in the pricing proposal/cost sheets. Contractor must provide toll-free telephone lines for reporting purposes.

SENTINEL RESPONSE

Sentinel offers the RF Patrol PHMU in two (2) models, one for Landline Communications using the participant's home phone line and another for Cellular Communications for participants without home telephone lines. The RF Patrol Cellular PHMU units use AT&T for communicating with Sentinel's monitoring system while the RF Patrol Landline utilizes a toll-free telephone line for reporting purposes.



- In the event of power disconnect or commercial outage the receiver must have a minimum of 24 hours internal, auto-recharging back-up battery to support complete continued functionality, including but not limited to detecting and reporting information.

SENTINEL RESPONSE

The RF Patrol PHMU receiver is designed with a **built-in auto-recharging backup battery that functions for up to 48 continuous hours of full operation** in the event of a commercial power failure at the participant's home or power cord disconnection. 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. Sentinel's proposed solution is also capable of retaining monitoring information in the event of loss of communication with the monitoring center. If telephone service or cellular communication is interrupted, the receiver will prioritize and store activity data in the receiver's non-volatile internal memory, automatically reporting the statuses immediately upon the return of telephone service.

- The receiver must record and report a tamper signal if the case is opened.

SENTINEL RESPONSE

The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts to the monitoring center with date and time stamps. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. **If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU.** In addition to PHMU tampers, the unit will detect and communicate all other alerts and notifications, including but not limited to PTX2 tampers, arrival and departures of the PTX2, loss and restoration of power or telephone service, and *HMU Late-To-Test*, indicative of impediments to the ability to report to the monitoring center. The RF Patrol PHMU home receiver unit is also equipped with features that generate alerts if the receiver is tampered or moved. 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 versus attempted relocation of the unit. If the unit is moved, a *HMU Tilt* alert is generated. Should the participant attempt to open the PHMU, the unit will generate an *HMU Tamper* alert.

- The receiver must continually attempt to dial into the Monitoring Center until it makes contact and downloads data or until power is disconnected or battery depleted.

SENTINEL RESPONSE

The PHMU will indefinitely continue to dial into the monitoring center until the device makes contact with the software and the data is downloaded or until power is disconnected or battery depletion. The PHMU will renew attempts to contact the monitoring center upon power restoration and will report all stored events in its memory upon connection with the monitoring center.



B. RF Software

B. Software Requirements.

- Web-based platforms must be accessible via desktop, tablet, and mobile devices.

SENTINEL RESPONSE

DNA is a secure web-based application that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year via commonly used web browsers (e.g., Google Chrome, Microsoft Edge, etc.) over a high-speed internet connection. The SentinelDNA Monitoring System is designed to simplify access and usage across modern browsers on workstation computers and laptops (Windows, Mac OS X, Linux) and any mobile device (iOS, Android). The DNA monitoring application is 100% Internet-based and agencies do not need to purchase, install, or download any custom hardware or software components, applications, or client requirements. This advanced application improves the overall management of program information providing direct access to monitoring data for all Sentinel staff as well as authorized Participating Entity personnel.

- Secure login with multi-factor authentication.

SENTINEL RESPONSE

Sentinel's proposed monitoring solution provides secure login with multi-factor authentication through a Two-Factor Authentication (2FA) that requires two distinct factors to verify a user's identity, such as a password and a one-time code. By enabling at least one of the methods below, the user's account will require 2FA to log in, and the user must authenticate when accessing the web application and mobile app via single sign-on (SSO). The monitoring solution supports two types of Authentication methods (1) Authenticator App and (2) Email.

- + **Authenticator App:** Authenticator Apps provide a Time-Based One-Time Password (TOTP), which is considered one of the more secure options compared to other two-factor authentication methods available. Many authenticator apps, such as Google Authenticator, Microsoft Authenticator, and FreeOTP, are available in the app stores for Android and iOS. Users must follow the Authenticator App's guidelines for installation and adding new accounts.
- + **Email OTP:** Another option available to users is to receive a one-time password (OTP) code in their email. Upon enabling this option, the system will send a code to the email address used to log in to the monitoring system account with their user ID.

- Automated notifications and alerts (via SMS, email, or in-platform) for violations such as zone breaches, tampering, or low battery, or any other alerts as defined by the Participating Entity.

SENTINEL RESPONSE

Sentinel's DNA web-based information system is also equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts / notifications and violations such as zone breaches, curfew breaches, tampering, or low battery, or any other alerts as defined by the Participating Entity. Violations can be prioritized to alert immediately or hold for a grace period. The **DNA Profile Manager** allows for automated (text/email/in-platform) notification of alerts as well as optional manual operator escalation/closed loop communication and sequencing. The Profile Manager also differentiates protocol changes within a single alert by time and day of the week. Please refer to the image below for Sentinel's **Notification Procedure** screen within DNA. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA NOTIFICATIONS PROCEDURE SCREEN

The screenshot shows a web application interface titled "Profile Viewer". It displays a notification procedure for "Do Not Pass Go Bonding (Version: 1)". The interface includes a sidebar with navigation icons and a main content area. The main content area shows a table of steps for the notification procedure, with columns for "State", "Action", "State Time", and "Next State". The steps are organized by day (Sunday and Monday) and time (00:00:00 - 23:59:59). The steps include "Auto Email and McApp", "Delay", and "McApp". The interface also includes a "Back to Profile Manager" button and a "Sign Out" button in the top right corner.

State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Step 2	Delay	10	Step 3
Step 3	McApp	0	

- Reporting capabilities with customizable fields, exportable in PDF, Excel, and CSV formats.

SENTINEL RESPONSE

SentinelDNA is designed and maintained entirely by Sentinel's in-house IT Team, thus reports with customized fields are available upon customer request. SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

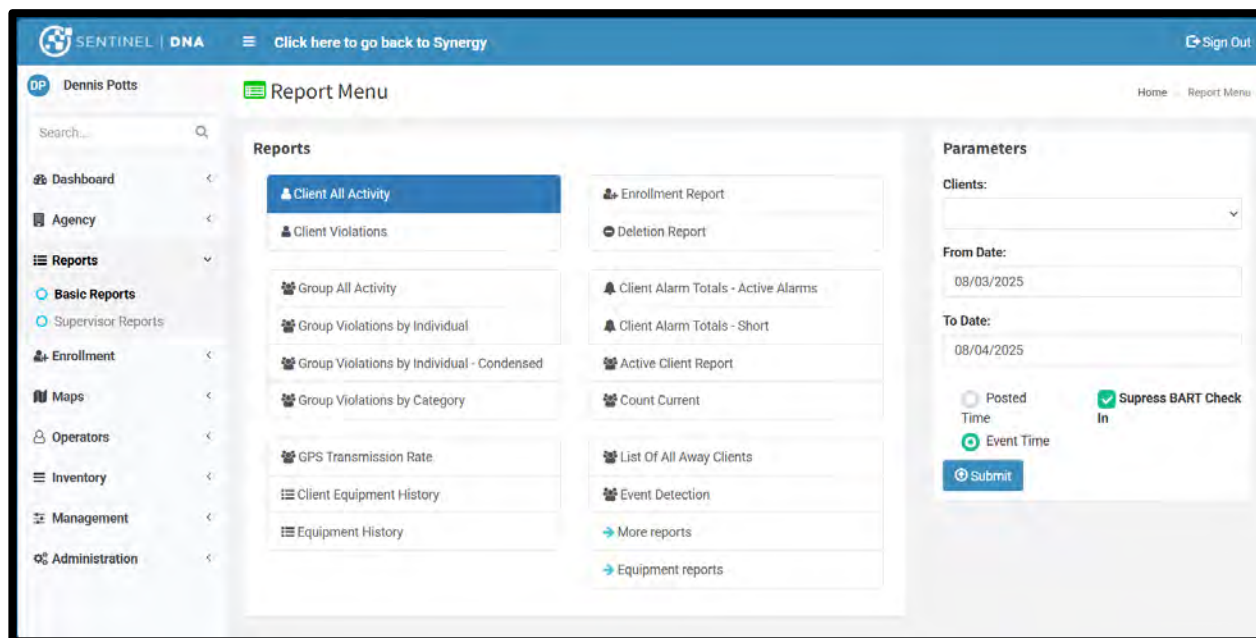
Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

DNA REPORT MENU SCREEN



If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

- Integration options with existing case management systems through APIs.

SENTINEL RESPONSE

Sentinel has developed and does support Application Programming Interfaces (APIs) to interface our SentinelDNA system with external systems. The Sentinel Software Development Team has extensive experience in developing and testing APIs, using best in class software development practices and tools such as Postman and REST Assured, and JMeter performance/load testing, to develop and test secure, robust and scalable API interfaces. Key technologies used include REST, JSON, JWT, and Webhooks.

Implementing an API would require an engagement between Sentinel and the contracting Entity's technical team(s) to understand the exact requirements, project scope, and infrastructure needs to implement the APIs and requested integration with a State's Offender Management System. Upon completion and agreement on the Project Scope Document, Sentinel would deliver the necessary API and/or integration for the contracting Entity and support our portion of this project to ensure system performance and uninterrupted data exchange.



- Audit trail and data retention in compliance with CJIS security requirements.

SENTINEL RESPONSE

The system's security and data-management framework are aligned with criminal-justice security expectations, providing full traceability for evidentiary purposes and long-term data retention requirements. Sentinel has designed the system, operations, and policies to align with CJIS requirements maintaining a complete audit trail for all device events, alerts, user actions, and monitoring results. Every action is time-stamped and retained according to strict data-integrity controls. All changes to participant or demographic information or monitoring data are saved within the system. Additionally, each employee has specific login credentials that permit Sentinel to perform detailed audits on user access to all participant records in the database to confirm that unauthorized changes have not been made. Additionally, our systems allow Participating Entities and their Supervisors to determine if an officer/user accessed any portion of our DNA system while monitoring the length of time the officer spent on the specific DNA module. This audit capability allows Supervisors to ensure officers are accurately reviewing tracking data and responding appropriately to program violations and participant activity.

- Role-based access controls for administrators, supervisors, and officers. The system must provide security features, which must prevent unauthorized individuals from accessing any information held by the Contractor. Secure access to the system must be maintained at all times.

SENTINEL RESPONSE

The Company enforces role-based access control (RBAC) for access to systems and data through centralized identity and access management. Access is granted only to pre-defined roles aligned to job responsibilities and the principles of least privilege and need-to-know, with documented approval from designated system/data owners. Privileged and administrative access is tightly restricted (including the use of MFA for privileged and remote access), and role assignments are reviewed at least quarterly and upon personnel or job changes, with prompt removal upon termination. Access provisioning, changes, and administrative actions are logged and monitored to support auditability and align with NIST SP 800-53 Moderate access control objectives (e.g., AC-2, AC-3, AC-5, AC-6).

Sentinel's DNA Monitoring Application offers hierarchy user levels that will allow the system administrator the ability to limit the tasks available to a particular user and/or group of users through role-based access controls. DNA will enable the designated system administrator to set access levels for each authorized user. Additionally, the system administrator will have the ability to establish access levels to specific caseloads or groups in any combination for authorized users. The system administrator will have the ability to secure and restrict, or alternately enable, access to clients and their information.

Secure access to the monitoring application is maintained at all times. The system is completely secure and uses state-of-the-art security measures. Login authentication is based on NIST SP 800-63-3 Digital Identity Guidelines to ensure secure access to the Monitoring System. Sentinel has employed the use of Single Sign-On (SSO) and Multifactor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.

The DNA Monitoring Application and Case Management Software were designed and are managed based on following NIST SP 800-53 requirements. Sentinel's security staff members have worked within the NIST 800-53 related standards and frameworks since 2009 and have received accreditation for NIST 800-53 compliance for past contracts and products. Sentinel conducts yearly penetration tests and vulnerability assessments to prioritize needed security improvements and remediations. Sentinel uses NIST 800-53 as the basis for information system policies to ensure federal standards are being met or exceeded. Sentinel partners with a 3rd party Security

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Operations Center (SOC) provider to achieve 24x7 Managed Detection and Response security monitoring of endpoints and network traffic. Sentinel's staff and security partner monitor security bulletins for emerging threats, 0-day vulnerabilities, and new CVEs with immediate priority for any needed remediation on Sentinel's system. Our SOC partner also provides Managed Risk Continuous Vulnerability Scanning of internal and external surfaces, as well as Managed Security Awareness training and phishing simulation for all employees. Sentinel's staff monitors dark web malicious actor blogs, forums, and databases for information and credentials related to Sentinel's systems.

Sentinel maintains an aggressive posture of cybersecurity diligence with an ongoing focus on continuous improvement of security operations. Components of Sentinel's applications are hosted in the Oracle Government Cloud Infrastructure. The U.S. Department of Defense, intelligence community, and federal civilian agencies rely on Oracle Government Cloud. Oracle US government cloud infrastructure meets the standards DoD DISA IL 5, 4, 2, FedRAMP-High, FIPS 140-2 for cryptographic modules and is VPAT section 508 compliant. All externally facing HTTPS endpoints require TLS 1.2 or TLS 1.3 and are configured to prefer AEAD cipher suites (AES-GCM/ChaCha20-Poly1305). This ensures strong session confidentiality (including AES-256 where negotiated), integrity protection, and forward secrecy, aligned with widely accepted modern TLS hardening guidance.

Sentinel protects the perimeter of the data center and office networks with Fortinet FortiGate firewalls with Intrusion Detection and Intrusion Prevention features enabled and tracked. Security and Traffic activity is logged and ingested into the Arctic Wolf SIEM for combined Managed Detection and Response (MDR). Combined with the SentinelOne XDR Endpoint Protection Platform that runs on all Sentinel's servers and employee workstations and laptops, the Arctic Wolf 24x7 operated MDR service provides 24x7 rapid detection and reaction to intrusions.

Sentinel does not allow vendors or 3rd party access to participant data. Sentinel staff and end users (agency officers) access participant data using multi-layered login passwords. All activities conducted in DNA are recorded with date, time stamp, and user credentials to provide audit capability, replay of events, and access to historical accuracy.

- The system must provide the capability for Participating Entity to download data and reports from the database, through secured internet access.
 - o Non-compliance with pre-determined curfews
 - o Client entry and exit at unauthorized times
 - o Tampering with the transmitter or any of its components
 - o Tampering with the receiver or any of its components
 - o Failure of the receiver to report at pre-determined times
 - o Loss and/or restoration of telecommunications
 - o Loss and/or restoration of alternating current (AC) power
 - o Detection of low power or battery malfunctions in the transmitter or receiver
 - o Movement of the receiver
 - o Detection of operating malfunctions in the receiver or transmitter

SENTINEL RESPONSE

SentinelDNA is a secure web-based information system that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year. The SentinelDNA Monitoring System is designed to simplify access and



usage across modern browsers on both workstation and laptop computers (Windows, Mac OS X, Linux) and mobile devices (iOS, Android). Additionally, users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves the overall management of program information providing direct access to monitoring data for all Participating Entity program personnel. Authorized users will have the ability to view and download data and reports through SentinelDNA:

- + **Non-compliance with pre-determined curfews:** The PHMU will report the participant's non-compliance with the pre-determined curfews established by the Participating Entity.
- + **Client entry and exit at unauthorized times:** The PTX2 ankle transmitter's encrypted signal is received by the PHMU receiver that reports to the monitoring system each time the participant enters and exits from the residence, including at unauthorized times.
- + **Tampering with the transmitter or any of its components:** The RFP Patrol PTX2 has dual tamper resistance capabilities including both fiber-optic and case tamper that are reported to the receiver, which sends the data to the monitoring system.
- + **Tampering with the receiver or any of its components:** The RF Patrol PHMU unit is designed to detect and report to the monitoring system multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts to the monitoring center with date and time stamps. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU.
- + **Failure of the receiver to report at pre-determined times:** In the event a PHMU does not report to the monitoring center in accordance with the device schedule, the SentinelDNA monitoring system will generate a "Late-To-Test" alert and monitoring protocols will be followed as defined by the Participating Entity to resolve the lack of communication event.
- + **Loss and/or restoration of telecommunications:** The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The unit retains all stored events and reports them to the monitoring system upon power restoration. Sentinel's proposed solution is also capable of retaining monitoring information in the event of loss of communication with the monitoring system. If telephone service or cellular communication is interrupted, the PHMU will prioritize and store activity data in the receiver's non-volatile internal memory, automatically reporting the statuses immediately upon the return of telephone service.
- + **Loss and/or restoration of alternating current (AC) power:** Sentinel's proposed RF Patrol solution is capable of retaining monitoring information in the event of loss of communications with the monitoring center. If communication is interrupted, the RF Patrol PHMU will prioritize and store activity data in the PHMU's non-volatile internal memory, which is capable of indefinitely storing approximately ninety (90) days' worth of events (approximately 1,024 events), including date and time stamps, automatically reporting the statuses to the monitoring system immediately upon the return of telephone service.
- + **Detection of low power in the transmitter or receiver:** The RF Patrol PTX2 (transmitter) will emit a low battery signal to the receiver/monitor with every communication. Under normal circumstances the PTX2 will communicate a low-battery message to the receiver and report it to the host server five (5) to seven (7) days prior to depletion. 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 in the event of a commercial power failure at the participant's home or power cord disconnection. If telephone service or cellular communication is interrupted, the receiver will prioritize and store activity data in the receiver's non-volatile internal memory, automatically reporting the statuses immediately upon the return of telephone service. All low power alerts are communicated to the monitoring system.
- + **Movement of the receiver:** 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



versus attempted relocation of the unit. If the unit is moved, a *Tilt In Motion* alert is generated. Should the participant attempt to open the PHMU, the unit will generate an HMU Tamper alert that will be reported to the monitoring system.

- + **Detection of operating malfunctions in the receiver or transmitter:** In Officer Mode the PHMU will measure and report on transmitter diagnostics including battery percentage, PTX2 range settings, and tampers status. The PHMU will also identify necessary steps to reconnect phone service during the installation process. The SentinelDNA monitoring system will monitor device connectivity and performance and report any missed communications as a result of device malfunction to the monitoring system.

- The Contractor must replace the radio-frequency EM system with any future updated and improved version of Contractor's or manufacturer's radio-frequency EM system at the request of the Agency and after successful field testing of the updated system.

SENTINEL RESPONSE

Sentinel will replace the radio-frequency EM system with any future updated and improved version of Sentinel's radio-frequency EM system at the request of the Agency and after successful field testing of the updated system.

- Contractor must have a notification policy for client violations that allows the Agency to establish distinct levels of security on a client-by-client basis. System must be designed with heightened emphasis on accuracy of RF signaling & speed of reporting. (Example: Use of 2-way radio transceivers instead of simple 1-way transmitter/receiver signaling).

SENTINEL RESPONSE

NOTIFICATION POLICY FOR CLIENT VIOLATIONS

Sentinel's user-friendly DNA monitoring application allows an agency to establish on a client-by-client basis, various Notification Protocol Procedures based on the risk level of the program participant and the intensity level needed for response and notification parameters needed on Key Alert Notifications.

ACCURACY OF RF SIGNALING & SPEED OF REPORTING

Sentinel's RF Patrol Radio Frequency (RF) electronic monitoring system is designed to determine whether 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. The ankle transmitter's signal is received by the paired home monitoring unit (landline or cellular based), which reports each time the participant enters and exits from the residence. The home monitoring unit also reports any changes to the ankle transmitter's status such as a low battery or tamper alert. Both the ankle transmitter and the home monitoring unit are equipped with anti-tamper features to ensure program integrity. The RF Patrol equipment is capable of continuously signaling, receiving, storing, and disseminating data (through landline or cellular communications) to the Sentinel monitoring center, all without any active involvement by the participant.

RF Patrol features a programmable leave window at the Participating Entity's direction; the standard leave window is five (5) minutes but can easily be remotely programmed to increase or decrease. Additionally, RF Patrol also features a programmable reporting window at the Participating Entity's direction; the standard reporting window is four (4) hours but can easily be remotely programmed to increase or decrease. The RF Patrol will immediately report transmitter status changes when in range of the RF Patrol unit (ie. Tamper, enters, leaves etc) The following list highlights some of the unique features of the proposed RF Patrol radio frequency monitoring solution:

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **Ease of Installation:** Installers can enroll the Personal Home Monitoring Unit (PHMU) after the Personal Transmitter (PTX2) is on the participant. Installers can complete PHMU enrollment through easy-to-follow prompts on the LCD screen in agency offices or at the participant's home. A telephone line is not required to complete the enrollment process.
 - + **Dual Transceiver, Two-way RF Link Approach:** Sentinel's unique dual transceiver approach incorporates both a transmitter and receiver in the home unit, as well as having both in the PTX2 bracelet.
 - + **Tamper Detection via Fiber Optic Strap:** RF Patrol has a highly advanced tamper detection scheme. It is a 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. This highly advanced technological design eliminates false "Body Tamper" alerts caused by older generation equipment.
 - + **Advanced Range Testing/Variable Range Setting:** Both the transmitter and the home unit indicate RF signal strength during range testing. This enables the Sentinel installers and/or Agency staff to perform accurate range testing at each installation, and the officer/installer can also determine the distance of the range setting in one of multiple distance settings.
 - + **Backup Battery with Non-Volatile Memory:** 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** in the event of a commercial power failure at the participant's home or power cord disconnection. 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 2,500 events, including date and time stamps.**
 - + **LCD Screen:** Provides alphanumeric informational prompts to both participants during supervision and Sentinel installers and/or Agency staff during installation/troubleshooting and monitoring status through the Setup Menu options.
 - + **LED Light:** LED light provides a clear indication of connection and/or pending alerts to assist during programming or troubleshooting.
 - + **Ability to Send a Text Message to the Home Unit:** The home unit can receive a text message from the Sentinel software for purposes of further communicating with the participant. Additionally, the program participant can acknowledge the message by touching a button on the home unit which transmits an acknowledgment signal to our monitoring system for inclusion in the participant activity.
 - + **Tilt/Motion Detection:** 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 versus attempted relocation of the unit.
 - + **Guest Bracelet Detection:** The system detects all Sentinel transmitters that come within range of the home unit. This unique feature detects and notifies officers if EM participants come in contact with one another and/or are comingling.
 - + **Group Monitoring Capabilities:** One (1) home unit can simultaneously monitor up to 50 transmitters, each with their own separate/unique curfew schedule.
- System must offer a secure means for the agency to simply and rapidly perform a range test to confirm signal coverage between the transmitter and receiver in the client's home.

SENTINEL RESPONSE

The RF Patrol monitoring system has a variable signal range between the PTX2 and PHMU, which is agency programmable on a per participant basis with three (3) settings as follows:

- + **LOW:** Approximately 50 feet

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **MEDIUM:** Approximately 100 feet
- + **HIGH:** Approximately 150 feet

PERFORMING A RANGE TEST

The Supervising officer can quickly and easily perform a range test by accessing the Officer Control module accessible directly from the PHMU by following the following steps:

- 1) Turn the PHMU Menu Key to the horizontal position;
- 2) Select RNG (range) from the Setup Menu;
- 3) Select TEST from the RNG Menu;
- 4) The LCD screen will display the words "Testing" and a negative (-) sign to the upper left and a positive (+) sign to the right of the LCD screen;
- 5) The transmitter will immediately begin to blink;
- 6) One (1) blink from the PTX2 indicates excellent range, two (2) blinks indicate good range, three (3) blinks indicate poor signal reception, and four (4) blinks indicate no signal reception (no longer in range);
- 7) Installer/Officer may walk with the participant to each section of the home during the range test to confirm range;
- 8) Once all areas of the home have been covered, select the [<] less than symbol to end the range test and return to the main menu;
- 9) Once the range test ends, the PTX2 will stop blinking, and;
- 10) Sentinel technicians will report to the appropriate Department the range setting applied during the installation process for each participant.

- System must be capable of varying the signal range between transmitter and receiver for each device to best match the risk of each client and the signaling coverage in each client's home.

SENTINEL RESPONSE

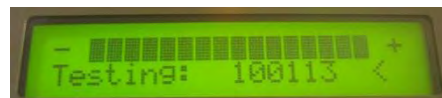
As shown above, Sentinel can offer the agency added confidence that its participants are reliably monitored while in their residences. Sentinel's RF Patrol equipment offers a unique feature that allows for visual range testing during the installation process. While installing the PHMU in the participant's residence, installers/officers have the capability to test the range between the PTX2 and the PHMU to ensure the agency will not receive false out-of-range alarms when the participant is inside their residence. This capability also assists the installers through ensuring that the range setting between the PTX2 and the PHMU is small enough to securely monitor the presence of the participant at his or her home during curfew hours.

The RF Patrol monitoring system has a variable signal range between the PTX2 and PHMU, which is agency programmable on a per participant basis 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



RF PATROL PHMU LED DISPLAYS
FOR RANGE TESTING



RF PATROL PHMU LED DISPLAY
FOR RANGE SETTING



- The receiver must perform internal diagnostics to determine if it is operating properly. These diagnostics must be reported by the receiver to the Monitoring Center computer and displayed in the event history.

SENTINEL RESPONSE

The RF Patrol PHMU (receiver) will perform internal diagnostics to determine if it is operating properly. The receiver recognizes and reports changes in device performance including power disconnect, low battery status, movement, and lack of response to incoming text messages. The receiver is also programmed to perform sanity check-ins on a regular basis further confirming operational status. These diagnostics are reported by the receiver to the Sentinel monitoring system and displayed in the event history.

- A Leave Window count-down timer exists within all RF receivers as a means of preventing false "Leave" events during short term signal loss while the transmitter is still in range. This Leave Window must be adjustable at the Agency's direction on a per unit/client basis. A Reporting Window count-down timer exists within all RF systems as a means of regularly confirming that the receiver is connected to the phone line and capable of reporting events (not disconnected from the phone line and unable to report, such as disconnected by a client before leaving range). This Reporting Window must be adjustable at the Agency's direction on a per unit/client basis.

SENTINEL RESPONSE

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 than any other vendor on the market. The Leave window is adjustable as needed by the Participating Entity for each participant.

The PHMU performs a "Sanity Check or Monitor Check-In" on a scheduled basis normally every 4-6 hours. (duration is programable based on Participant Entity preference). These scheduled check-ins ensure the device remains properly installed with commercial power and communication status confirmed. In the event a PHMU does not report to the monitoring center in accordance with the device schedule, the SentinelDNA monitoring system will generate a "Late-To-Test" alert and monitoring protocols will be followed as defined by the Participating Entity to resolve the lack of communication event.

- When landline services are being used, the receiver must detect, and report events related to the disconnection and reconnection of the electrical power and telephone line.

SENTINEL RESPONSE

The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing.

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 people 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. This feature is particularly important for 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.



The unit retains all stored events and reports them to the monitoring center upon power restoration. Sentinel's proposed solution is also capable of retaining monitoring information in the event of loss of communication with the monitoring center. If telephone service or cellular communication is interrupted, the PHMU will prioritize and store activity data in the receiver's non-volatile internal memory, automatically reporting the statuses immediately upon the return of telephone service.

- When landline services are being used, the receiver must incorporate at least 1000 events non-volatile memory to store events (with date and time of occurrence) at times when the phone line is not available and continually attempt to report them until reporting has been successful.

SENTINEL RESPONSE

The RF Patrol PHMU has an internal non-volatile memory capable of indefinitely storing approximately 90 days of monitoring events (approximately 2,500 events), including date and time stamps when phone service is not available. The unit retains all stored events and continually attempts to report to the monitoring center until such time as phone service is restored or, in cases where cellular units are being used, restoration of cellular connectivity has occurred.

- When landline services are being used, the receiver must allow use with any brand or make of telephone line including touch tone, broadband, and DSL and VoIP.

SENTINEL RESPONSE

The RF Patrol electronic monitoring solution will include either landline (digital, broadband, DSL, VoIP compatible) or cellular-enabled home monitoring unit. The RF Patrol Landline PHMU units have proven functional on standard RJ-11 telephone lines, including touchtone, without interruption and when other devices such as cable, satellite, or DSL and VoIP service are working on or with the participant's landline.

- The receiver must be able to receive and record any client status change, such as when the client entered or left the residence, as well as the working condition and tamper status of the receiver and the transmitter. The receiver must have the ability to record the actual time of occurrence.

SENTINEL RESPONSE

The RF Patrol PHMU will receive and record any client status change, such as when the client entered or left the residence, as well as the working condition and tamper status of the receiver and the transmitter. The PHMU receiver will record the actual time of occurrence with date and time stamp available in the client activity report.

- The receiver must communicate the client's status to the Monitoring Center Computer immediately in the event of curfew violations (at expiration of leave window) (including the transmitter returning within range) or transmitter tampers.

SENTINEL RESPONSE

The RF Patrol PHMU (receiver) will immediately communicate the client's status to the monitoring system in the event of curfew violations (at expiration of leave window) (including the transmitter returning within range) or transmitter tampers.



- The receiver must notify the Monitoring Center of any tamper attempts to the receiver itself as well as AC power source problems or disconnects. The software must detect and report communication disruptions resulting in interrupted/delayed reporting. All messages must be time and date stamped with actual time of occurrence.

SENTINEL RESPONSE

The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts to the monitoring center with date and time stamps. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU. In addition to PHMU tampers, the unit will detect and communicate all other alerts and notifications, including but not limited to PTX2 tampers, arrival and departures of the PTX2, loss and restoration of power or telephone service, and *HMU Late-to-Test*, indicative of disruptions resulting in interrupted/delayed reporting to the monitoring center.

The PHMU performs a "Sanity Check or Monitor Check-In" on a scheduled basis normally every 4-6 hours. (duration is programable based on Participant Entity preference). These scheduled check-ins ensure the device remains properly installed with commercial power and communication status is confirmed. In the event a PHMU does not report to the monitoring center in accordance with the device schedule, the SentinelDNA monitoring system will generate a "Late-To-Test" alert and monitoring protocols will be followed as defined by the Participating Entity to resolve the lack of communication event. All events are submitted with date and time stamp at the actual time of occurrence.

The RF Patrol PHMU home receiver unit is also equipped with features that generate alerts if the receiver is tampered or moved. 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 versus attempted relocation of the unit. If the unit is moved, a *Tilt In Motion* alert is generated. Should the participant attempt to open the PHMU, the unit will generate an *HMU Tamper* alert. All events are submitted with date and time stamp at the actual time of occurrence.

C. RF Customer Support & Training

C. Customer Support and Training

- The Contractor must provide a dedicated account representative.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

As a leading provider of electronic monitoring services and as a NASPO ValuePoint contractor for more than 25 years, Sentinel has established processes and protocols to effectively deliver services via NASPO ValuePoint agreements. Sentinel will continue to ensure familiarity with the Master Agreement including all terms and pricing.

The NASPO ValuePoint Agreement will receive full attention of Sentinel's Senior Leadership team as evidenced by the fact Sentinel is appointing Mr. Mike Dean, Sentinel's Senior Vice President of Sales as the point of contact for the NASPO ValuePoint Master Agreement.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Mr. Dean oversees all Sentinel sales personnel and manages the company's cooperative purchasing agreements. With over 33 years in the electronic monitoring industry overseeing sales and contracting for some of the largest electronic monitoring providers, including BI Incorporated, 11 years, G4S Justice Services, 7 years, and Sentinel for the past 14 years, Mr. Dean has unparalleled expertise in collaborating with Federal, State, and Local Governments, developing electronic monitoring programs and leveraging cooperative purchasing to the benefit and convenience of government agencies.
- + Mr. Dean has worked directly with procurement departments negotiating Participating Addendums and reviewing contractual requirements for entities that makes him an exceptional subject matter expert and primary point of contact for the NASPO ValuePoint Cooperative Purchasing Agreement. Mr. Dean holds a Bachelor Agreement in Criminal Justice, from the University of Cincinnati, and as Senior Vice President of Sales, Mr. Dean is strategically positioned to champion the NASPO ValuePoint agreement. He will provide corporate oversight for the agency's participating addendums, programs and purchasing department, while also facilitating all post-award implementation adjustments required for this contract.

Mr. Dean will work closely with the Sentinel Field Operations Team and have complete support from our Chief Operating Officer, Mr. Darryl Martin. Mr. Martin has been overseeing the delivery of electronic monitoring services to the NASPO ValuePoint Agreements for more than 25 years. Mr. Martin will exercise all Sentinel departments and employee base of more than 280 to ensure complete compliance with the Master Agreement including the following resources that stand ready to continue providing services.

Mrs. Melissa Staff, Sentinel's Senior Vice President of Field Operations, is responsible for the management and oversight of our Regional Account Management team as well as Sentinel's national network of customer support and branch office personnel. Her team manages the day-to-day needs of our benchmark offender-funded programs as well as providing customer service to our agency-funded contracts across the United States. **A dedicated account representative will be assigned to each Participating Agency for the duration of contract operations.** The Sentinel account representative will be responsible for:

- + Account retention;
- + Being the main liaison between the Customer and Sentinel;
- + Providing consultative account management practices to government channel accounts in their region to ensure best practices are in place;
- + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
- + Introduction and socialization of hardware and software offerings that may benefit the Customer;
- + Conducting training and overseeing the implementation; and
- + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.

- The Contractor must provide support functions 24/7/365.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained technicians and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

Our monitoring centers are staffed 24 hours a day, 7 days a week with live staff including a supervisor always on duty and certified operators cross-trained to support our suite of supervision services and monitoring products. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year. **There is no subcontracting of any of our proposed monitoring services.**

Sentinel provides access to designated **Help Desk** staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. Sentinel provides toll-free telephone access, toll-free fax line, and email access to over 60 operators and customer service representatives, available to officers 24 hours a day, 7 days a week, 365 days a year, who can resolve most technical problems over the telephone or through remote diagnostics.

Sentinel strives to resolve all customer inquiries promptly and on first contact. Each monitoring center operator has the expertise to easily identify, explain, and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert and changing a participant's schedule.

In addition, this specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

- The Contractor must provide toll free access to customer support/monitoring center.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained operators and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

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

In the unlikely event that problem solving requires a higher-level of involvement, Sentinel's customer service is equipped with all necessary computer equipment and staffed by experienced technicians, as well as the engineers who developed the system technology, who can quickly analyze and resolve the problem.



- The Contractor must provide initial start-up training that must include but not be limited to the following:
 - o The enrollment of clients into the software system.
 - o The installation, use, de-installation, and cleaning of the equipment.
 - o The generation and interpretation of data/monitoring reports.
 - o Accessing/using Contractor's technical support/help menus and monitoring center.

SENTINEL RESPONSE

Sentinel understands that training and customer service are crucial to the success of any electronic monitoring program, and Sentinel is dedicated to meeting those needs. Sentinel agrees to provide the initial training session and ongoing training, including all manuals, concerning the implementation and management of the monitoring program as determined by the contract. Sentinel is committed to establishing a partnership over the term of the contract to ensure that all staff members are fully and properly trained. Training is offered for the life of the program as outlined in the monitoring services agreement at no additional cost.

Sentinel's training philosophy for our instructor-led courses can be a combination of respondent training as well as train-the-trainer if so desired by the Participating Entity. We work to provide all training for our customers based on their individual programmatic needs and thus will work with the Participating Entity to develop and deliver a training format that provides the best solution for each training location. Sentinel's standard training minimally includes the following items: installation and de-installation of equipment; maintenance and cleaning of equipment; use of web-based information system including procedures for enrollment and curfew changes as well as the generation and interpretation of reports; troubleshooting monitoring problems; accessing our technical support and monitoring center; and any additional training as needed to remain current on monitoring equipment and web-based information system.

Sentinel's implementation team will train all agency personnel assigned to the program prior to deployment and as needed for changes to the system, equipment, web-based information system, or personnel, for the duration of the program as directed by the contract. Our standard training protocol includes demonstration, discussion, and hands-on sessions on the following topics:

- + All RF, GPS, Alcohol Monitoring equipment, and client app solutions (use, installation, removal, and troubleshooting)
- + Enrollment (enrollment, deactivation, and the setting of all monitoring parameters including curfew schedules and GPS zones)
- + Tracking and monitoring of participants
- + Alarm processes and resolution procedures (agency-specific protocols)
- + Notification processes and reports (agency-specific protocols)
- + Monitoring System (complete instruction on the use of the web-based information system including, but not limited to, participant enrollment, modifications, reports, schedules, advanced automated analytics, location review, and deactivations)
- + Interpretation of Monitoring Reports (review, define and interpret daily monitoring activity, and Glossary of Terms/definitions)
- + Mobile Application (complete instruction on the use of the Mobile App including, but not limited to, participant information modifications, schedules, location review, device command initiation, field contacts, equipment inventory, and reports/activity review)
- + Accessing Technical Support and Help Desk Services (contact information and access to training support materials)



- The Contractor must provide materials and brochures on the use of the equipment and system.

SENTINEL RESPONSE

Sentinel will provide all user guides, user manuals, brochures, PowerPoint presentations, reference guides, and training videos on the use of the equipment and system for each Participating Entity. Additionally, Sentinel will provide instruction and hand-out material for agency staff to instruct program participants on the use, care, and charging of the equipment.

- The Contractor must provide on-going and supplemental training offerings either on-site or via web-based programs at a minimum of once (1) per year after the initial start-up training offerings or on an as needed basis, based on any significant changes to the Contractor provided equipment and/or technology.

SENTINEL RESPONSE

In addition to the initial training and set up process with a representative on location, the Sentinel Training Department offers either on-site or via webinar training sessions for customers and staff at a minimum of once (1) per year after the initial start-up training offerings, on an as-needed basis, or based on any significant changes to equipment and/or technology. This training is offered for all technologies and services including those proposed herein. It is important to note that Sentinel's webinar training sessions involve interactive voice plus visual contact with a live Sentinel expert trainer, therefore trainees can ask questions and engage in discussion with the trainer as part of any webinar.

Training and webinars are offered at no additional cost to the Participating Entity based on internal training calendars, individual training needs, and scheduled on demand. Webinars are conducted based on contract specifications and/or training needs and can include training on equipment, services, software, web-based system changes, and/or updates. Training is offered for the life of the program as outlined in the Master Agreement. At any time, a Participating Entity can contact our Help Desk for additional support to ensure they are maximizing the technology solution to its fullest potential.

Remaining Category 2: RF Questions

2. Describe the hardware you propose to meet the requirements of the SOW, including battery life.

SENTINEL RESPONSE

Sentinel's RF Patrol™ Radio Frequency (RF) electronic monitoring technology 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 is an option for populations where GPS is not required, and curfew compliance meets the agency's needs.** This equipment is capable of continuous 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.



The RF Patrol radio frequency electronic monitoring system is comprised of a tamper-evident ankle transmitter and a home monitoring unit. The ankle transmitter's encrypted signal is received by the home monitoring unit (landline or cellular based), which reports each time the participant enters and exits from the residence. The home monitoring unit also reports any changes to the ankle transmitter's status such as a low battery or tamper alert.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The RF Patrol PTX2 is powered by a lithium thionyl-chloride, 3.6V, 750 milliamp hours (mAh) battery pack that is designed for a continuous operating life of 24 months, proactively replaced by Sentinel at an 18-month interval and has a four (4) year shelf life. The RF Patrol PHMU is equipped with a 48-hour backup battery. 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 (approximately 2,500 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.

Both the ankle transmitter and the home monitoring unit are equipped with anti-tamper features to ensure program integrity. The RF Patrol transmitter is waterproof, sealed, and designed with fiber-optic tamper detection technology to report any tamper attempts. The RF Patrol home monitoring unit is designed with a tamper detection feature if the case is compromised, along with a built-in multi-day battery back-up, and a motion sensor to detect if the unit is relocated to a different location.

Properties of the RF Patrol Transmitter and Paired Receiver: 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. The PTX2 can be quickly attached to the participant's ankle in under five (5) minutes and easily replaced in the field by Agency officers.



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. The bracelet records and reports each tamper as a separate event alerting the agency of a participant's tamper frequency level.

The RF Patrol home unit (PHMU) is 7.5 x 8.6 x 1.7 inches and weighs less than one (1) pound, making it one 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 phone connection, and a cellular modem incorporated into the internal architecture. The PHMU is available in both landline and cellular models to accommodate all participants, even those without home phone lines and uses the AT&T cellular network for communicating with Sentinel's monitoring system.



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 PTX2 bracelets in the vicinity of the home unit.

—IMPORTANT SENTINEL ADVANTAGE—

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

Tamper Detection Features: RF Patrol has a highly advanced tamper detection scheme. The PTX2 transmitter bracelet's sophisticated fiber-optic strap design uses light rather than a conductive circuit to ensure the participant cannot tamper with the unit without the generation of a tamper alert. The 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 while in range. Sentinel PTX2 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 virtually eliminates concern for "*false tamper*" alerts created by other vendors through normal usage at home or in typical work environments.

The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. The PHMU housing is made of high impact ABS plastic, is tamper resistant and reports tamper alerts to the monitoring center with date and time stamps. The unit has non-commercially available security hardware sealed with tamper evident tape to reflect visual signs of tampering. If a participant opens the case of the unit providing access to the internal circuitry, the unit's internal architecture has an internal tamper switch that will detect and report tampering of the internal PHMU. In addition to PHMU tampers, the unit will detect and communicate all other alerts and notifications, including but not limited to PTX2 tampers, arrival, and departures of the PTX2, loss and restoration of power or telephone service, and *HMU Late-To-Test*, indicative of impediments to the ability to report to the monitoring center. The RF Patrol PHMU home receiver unit is also equipped with features that generate alerts if the receiver is tampered or moved. 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 versus attempted relocation of the unit. If the unit is moved, a *Tilt In Motion* alert is generated. Should the participant attempt to open the PHMU, the unit will generate an *HMU Tamper* alert.

Unique Feature of the RF Patrol Solution: The following list highlights some of the unique features of the proposed RF Patrol radio frequency monitoring solution:

- + **Ease of Installation:** Installers can enroll the Personal Home Monitoring Unit (PHMU) after the Personal Transmitter (PTX2) is on the participant. Installers can complete PHMU enrollment through easy-to-follow prompts on the LCD screen in agency offices or at the participant's home. A telephone line is not required to complete the enrollment process.
- + **Dual Transceiver, Two-way RF Link Approach:** Sentinel's unique dual transceiver approach incorporates both a transmitter and receiver in the home unit, as well as having both in the PTX2 bracelet.
- + **Tamper Detection via Fiber Optic Strap:** RF Patrol has a highly advanced tamper detection scheme. It is a 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. This highly advanced technological design eliminates false "Body Tamper" alerts caused by older generation equipment.
- + **Advanced Range Testing/Variable Range Setting:** Both the transmitter and the home unit indicate RF signal strength during range testing. This enables the Sentinel installers and/or Agency staff to perform accurate range testing at each installation, and the officer/installer can also determine the distance of the range setting in one of multiple distance settings.
- + **Backup Battery with Non-Volatile Memory:** 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** in the event of a commercial power failure at the participant's home or power cord disconnection. 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 2,500 events, including date and time stamps.**

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **LCD Screen:** Provides alphanumeric informational prompts to both participants during supervision and Sentinel installers and/or Agency staff during installation/troubleshooting and monitoring status through the Setup Menu options.
- + **LED Light:** LED light provides a clear indication of connection and/or pending alerts to assist during programming or troubleshooting.
- + **Ability to Send a Text Message to the Home Unit:** The home unit can receive a text message from the Sentinel software for purposes of further communicating with the participant. Additionally, the program participant can acknowledge the message by touching a button on the home unit which transmits an acknowledgment signal to our monitoring system for inclusion in the participant activity.
- + **Tilt/Motion Detection:** 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 versus attempted relocation of the unit.
- + **Guest Bracelet Detection:** The system detects all Sentinel transmitters that come within range of the home unit. This unique feature detects and notifies officers if EM participants come in contact with one another and/or are comingling.
- + **Group Monitoring Capabilities:** One (1) home unit can simultaneously monitor up to 50 transmitters, each with their own separate/unique curfew schedule.

3. Describe your software system (web-based applications, smart phone applications).
Describe unique design features that ensure accuracy and/or speed of reporting.

SENTINEL RESPONSE

WEB-BASED SOFTWARE SYSTEM

SentinelDNA is Sentinel's in-house proprietary monitoring system designed exclusively for the electronic monitoring industry. **The strength of SentinelDNA resides in the system's ability to monitor Radio Frequency, Breath Alcohol, GPS technology and Mobile Applications. The RF Patrol device benefits from all of the SentinelDNA features discussed in the GPS section of this RFP response.** For brevity purposes we will outline only the additional items related to RF monitoring and refer the reader back to the Category 1: GPS subsection "**Remaining Category 1: GPS Questions**" (page 86) for more information about the GPS capabilities.

SentinelDNA™ (DNA) is a secure web-based information system that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year. No software components, applications, or client requirements need to be installed by the agency. The SentinelDNA Monitoring System is designed to simplify access and usage across modern browsers on both workstation and laptop computers (Windows, Mac OS X, Linux) and mobile devices (iOS, Android). Additionally, users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves the overall management of program information providing direct access to monitoring data for all authorized agency program personnel.

Designed in-house by Sentinel engineers, DNA can be customized to include all required reports, notification procedures and optional escalation alert sequencing. Moreover, this powerful and easy to use platform will provide the agency with customizable features and benefits not available from other monitoring solutions. DNA makes it easy for officers to access real time information about individual participants or their whole caseload from a secure environment (username and password are required for login). Designed with the needs of end-users in mind, DNA uses a straightforward, intuitive user interface that allows users to efficiently complete all monitoring tasks including:

- + Enroll a participant
- + Create/edit schedules
- + View, create notes
- + Perform data management administration
- + Create and edit zones (inclusion and exclusion)
- + Adjust tracking rate plans

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Clear events and alerts
- + Locate participants
- + Send custom messages to participant(s)
- + Store and view demographic information
- + Alert processing and advanced triage notification
- + Perform analytics including Point Pattern Analysis and Event Detection
- + Verify and document even contact with participants while in the field
- + Inventory Management including Equipment Recovery Dashboard
- + Review device battery status and charging events
- + Create and print reports
- + Store and view photos and documents
- + Victim assignment and notification
- + Perform audits

Sentinel's monitoring system records all data with a historical transaction record and is stored/archived for retrieval/backup in a database when requested by agency personnel. SentinelDNA Monitoring Application maintains a permanent searchable and reportable record in the form of a: 1) Client Audit Report; and 2) User Audit Report. In addition, all monitoring events and notifications are logged with date and time stamp and are also available for auditable review.

Sentinel's DNA platform offers advanced features and capabilities unavailable in other monitoring and tracking platforms:

- + **Sentinel Designed and Owned:** Engineered, maintained, and monitored exclusively by Sentinel allowing for system personalization as required by the Participating Entity.
- + **Login Authentication:** The system is completely secure and uses state-of-the-art security measures. Sentinel has employed the use of Single Sign-On (SSO) and Multifactor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.
- + **Client Dashboard** provides all participant data on one easy-to-read screen. Using straightforward alert icons, the DNA Client Dashboard provides an easy to read at-a-glance interface that allows users to quickly see the status of each participant. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, location information (via mapping), current equipment status, current battery status, as well as zones and curfew schedules.
- + Advanced **automated screen resizing** enables DNA to be accessed by desktops, laptops, tablets and by most leading smartphone browsers without the need to download custom applications.
- + **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 system allows DNA to provide a participant's current location and location history **via Google's map view, satellite/aerial view, bird's eye view, and street view**.
- + **Scheduling** DNA allows users to view and modify all participant curfew schedules and zone schedules as well as view and print monitoring activity reports for all participants. **DNA has the capability to create permanent and temporary schedules and to copy and paste a schedule from one day to the next.** All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.
- + Advanced and extensive **Report Library**, which can be increased at any time at no additional cost. The **Report Library** provides access to all standard system-generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Each data field within the entire information system can be queried to generate necessary report information. **Users have the option to view, save, and/or print data and/or reports from the system.**
- + **Advanced Inventory Control Module** enabling officers/installers 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 equipment orders online via DNA.
- + **DNA Mobile Application** provides officers with mobile access to review participant monitoring data via a smartphone or tablet. Sentinel has developed our DNA Mobile Application for officers to **perform field**

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



services and data management work such as data/schedule changes, equipment changes, de-installations, tracking review, current location requests, etc. from any smartphone or tablet.

- + Optional **Sentinel DNA Case Management Module** that is enabled within our existing DNA monitoring application that handles offender caseloads as well as all the data and interactions that comprise an offender population, including the accurate and consistent posting of client payments.
- + Sentinel has a proven **DNA Application Programming Interface (API)** and is prepared to coordinate with the Participating Entity's Information Technology (IT) to implement an interface between the Participating Entity's systems and Sentinel's DNA application whereby common participant data elements and monitoring data may be automatically pushed/pulled between the two (2) systems, thereby increasing officer efficiency by mitigating the need for duplicate keyed entry into both systems.

Client Dashboard. DNA utilizes an advanced **Client Dashboard** feature that provides authorized agency staff with the flexibility to view all or selected subsets of their entire caseload in near 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 each participant without having to research every record to confirm who is in violation and who is not. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, *location* information (via mapping), *current equipment status*, *current battery status*, as well as *zones* and *schedules*.

DNA CLIENT DASHBOARD

Name	OID	Type	Equipment	Compliance	Battery	Profile	Officer
Test Group: Advocate App PT, Carlos	ID8768866	GPS3			4%	Web Only	Dennis Potts
Test Group: Advocate App Vic, Carlos M	ID8768872	VAPP			96%	Web Only	Dennis Potts
Dell, Dee	ID8733643	CM				Web Only	Justin Case
Doe, Jill	ID8718393	VAPP			79%	Web Only	LauraZZZ ZZZDennison
Doe, John	ID8717208	CM				Web Only	LauraZZZ ZZZDennison
HELM Tester, AT&T OM500	ID8719830	GPS3				HELM GPS Testers	Training Department
HELM TESTER, RF BART	ID8748994	RF/BART				Web Only	Marielena Tejeda
HELM Tester, Verizon OM500	ID8693586	GPS3				HELM GPS Testers	Training Department
Jones, David	ID8741640	GPS3			5%	Web Only	LauraZZZ ZZZDennison
Kelso, Jackie (Install)	ID8719098	CM				Web Only	LauraZZZ ZZZDennison
Smurf, Papa	ID8732145	CM				Web Only	Christy Suazo
TCP Test	ID8742997	GPS3				Web Only	LauraZZZ ZZZDennison
TCP Level 3, Christy	ID8758249	GPS3				Christy Tester profile	Vanessa Gonzalez
Wonka, Jenna	ID8735419	CM				Web Only	Training Department

Quick Sorting Feature: Authorized users can refine the information displayed on the dashboard by clicking on one of the columns which then sort the participants based on that parameter. **This allows agency staff to quickly view participants by type of monitoring, by alert, or even by battery percentage.** In addition to sorting the information by column, filter icon buttons (shown below) are displayed at the top right of the dashboard, which allow the user to filter participants based upon the selected status/alert criteria.



Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

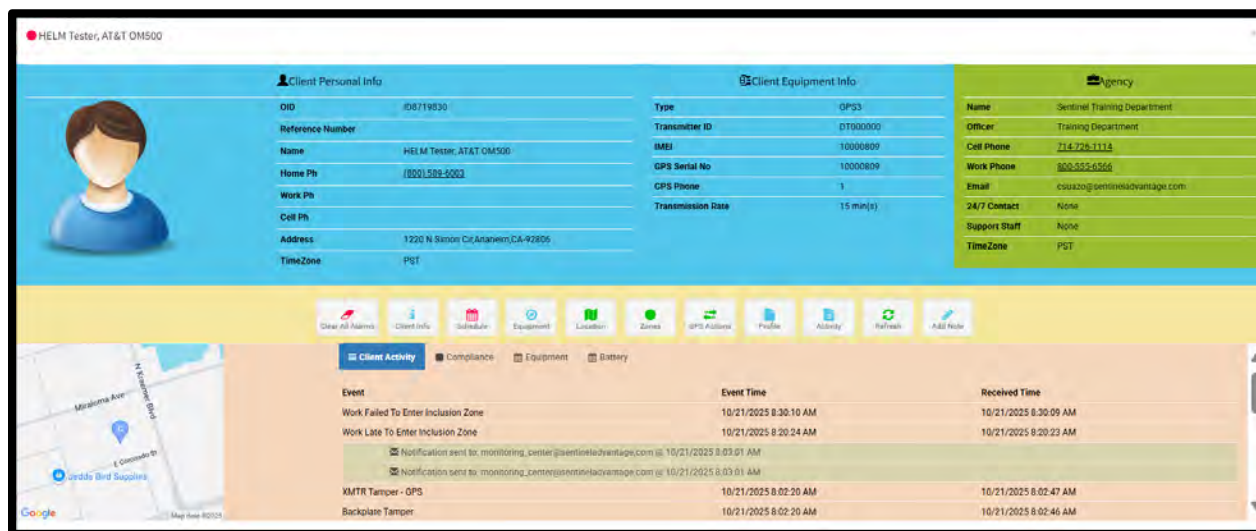


For example, by selecting the Tamper icon , only those participants with a Tamper alert are displayed on the dashboard. **This allows agency personnel to quickly review alert information each morning and prioritize contact with participants to better manage their caseload.** Below the sort icons, DNA has a local search option (shown below) to make it easy to refine the dashboard display to specific populations or participants with specific first/last names.



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

DNA CLIENT ACTIVITY SCREEN



HELM Tester, AT&T OM500

Client Personal Info		Client Equipment Info		Agency	
OID	056719830	Type	GPS	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT900000	Officer	Training Department
Name	HELM Tester, AT&T OM500	IMEI	10000809	Cell Phone	714-725-1114
Home Ph	(800) 582-5002	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csazog@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Senior Ct, Anaheim, CA 92805			Support Staff	None
Timezone	PST			Timezone	PST

Client Activity | Compliance | Equipment | Battery

Event	Event Time	Received Time
Work Failed To Enter Inclusion Zone	10/21/2025 8:30:10 AM	10/21/2025 8:30:09 AM
Work Late To Enter Inclusion Zone	10/21/2025 8:20:24 AM	10/21/2025 8:20:23 AM
Notification sent to: monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
Notification sent to: monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
KMTR Tamper - GPS	10/21/2025 8:02:20 AM	10/21/2025 8:02:47 AM
Backplate Tamper	10/21/2025 8:02:20 AM	10/21/2025 8:02:46 AM

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. **This provides all the important participant information on one screen.**

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT EQUIPMENT STATUS SCREEN

Client Personal Info		Client Equipment Info		Agency	
OID	ID8719836	Type	GPS3	Name	Sentinel Training Department
Reference Number		Transmitter ID	DT000000	Officer	Training Department
Name	HELM Tester, AT&T QM500	IMEI	10000809	Cell Phone	714-726-1114
Home Ph	(800) 589-6003	GPS Serial No	10000809	Work Phone	800-555-6566
Work Ph		GPS Phone	1	Email	csuazo@sentineladvantage.com
Cell Ph		Transmission Rate	15 min(s)	24/7 Contact	None
Address	1220 N Simon Ct, Anaheim, CA 92805			Support Staff	None
TimeZone	PST			TimeZone	PST

As illustrated in the Equipment Status screen image above, Officers can quickly view if there is a device issue without wasting time.

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

Name	OID	Reference Number	Type	Equipment	Compliance
[Redacted]	ID5737143	02972212	RF	[Redacted]	[Redacted]
[Redacted]	ID5806907	02443375	RF	[Redacted]	[Redacted]
102 Victim	ID5803916		GPS3	[Redacted]	[Redacted]
109 Victim	ID5805869		GPS3	[Redacted]	[Redacted]
106 Victim	ID5783386		GPS3	[Redacted]	[Redacted]

Real Time Scheduling, Zones, Authorized users access our DNA Web-Based 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 as well as view and print monitoring activity reports for all participants. All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.

DNA displays participant location information with a date and time stamp for each event. This chronological display is provided on screen as well as in printed report format.

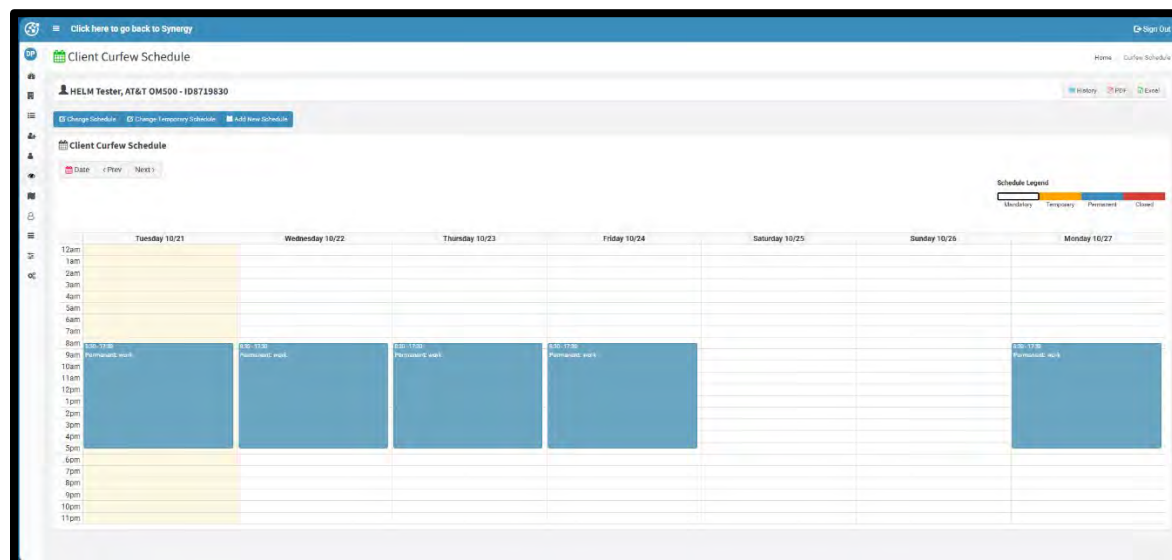
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Scheduling. During program enrollments, staff enter curfew/zone schedules and/or inclusion and exclusion zone schedules for each program participant in our DNA web-based system. SentinelDNA schedules allow supervising entities to select specific periods when a participant is required or is not allowed to be within the residence (or range of the RF Patrol device). All leave and enter events are triggered by when the participant leaves the range of his/her PHMU. Each exit from, and entry to, the residence) is reported by the PHMU, and the DNA web-based system automatically compares the activity to the established schedule. This activity verification is continuously performed by DNA, which thereby always ensures the monitoring of each program participant. **DNA also has the capability to create permanent and temporary schedules for both GPS and RF clients and to copy and paste a schedule from one day to the next.**

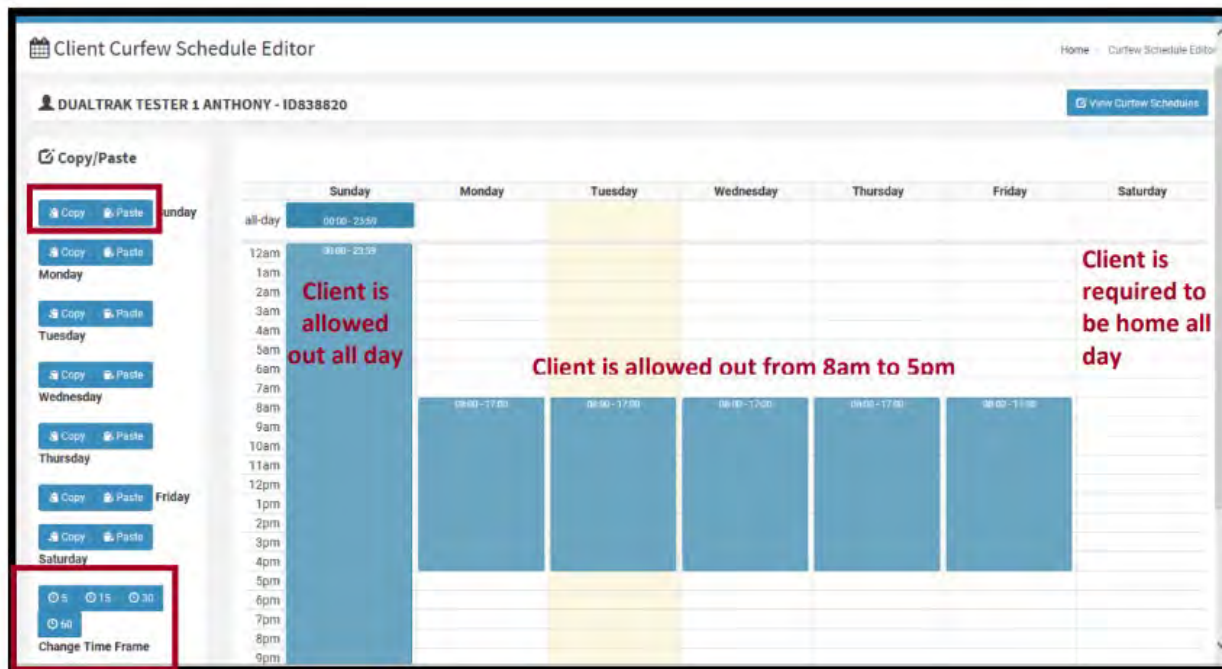
DNA CLIENT CURFEW SCHEDULE SCREEN IMAGE



Schedules within DNA define specific time periods when the client is required to be home or is permitted to leave his/her home. If no schedule is assigned to the client, the default setting for each client schedule is "Closed" – meaning the client is not permitted to leave the residence.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Accuracy of RF Reporting. Speed of reporting is typically defined as the round-trip delay of a command and is largely dependent on the underlying radio and cellular network. Under normal operating conditions, this delay is minimal. When RF Patrol is integrated with the DNA platform, the system provides unique capabilities that support both accuracy and reporting speed, including required acknowledgements within DNA to ensure data integrity, while leveraging cellular networks to enable timely transmission and reporting.

An additional design feature that contributes to system accuracy is the inclusion of RF signal level measurement within the PHMU. This capability allows the system to assess the strength of the RF signal, which directly correlates to data reliability and accuracy. Stronger RF signal measurements enable more accurate interpretation of events and environmental conditions, making this a unique feature that enhances overall system accuracy.

Reporting Module and Notification Procedures. SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system.. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



—IMPORTANT SENTINEL ADVANTAGE—

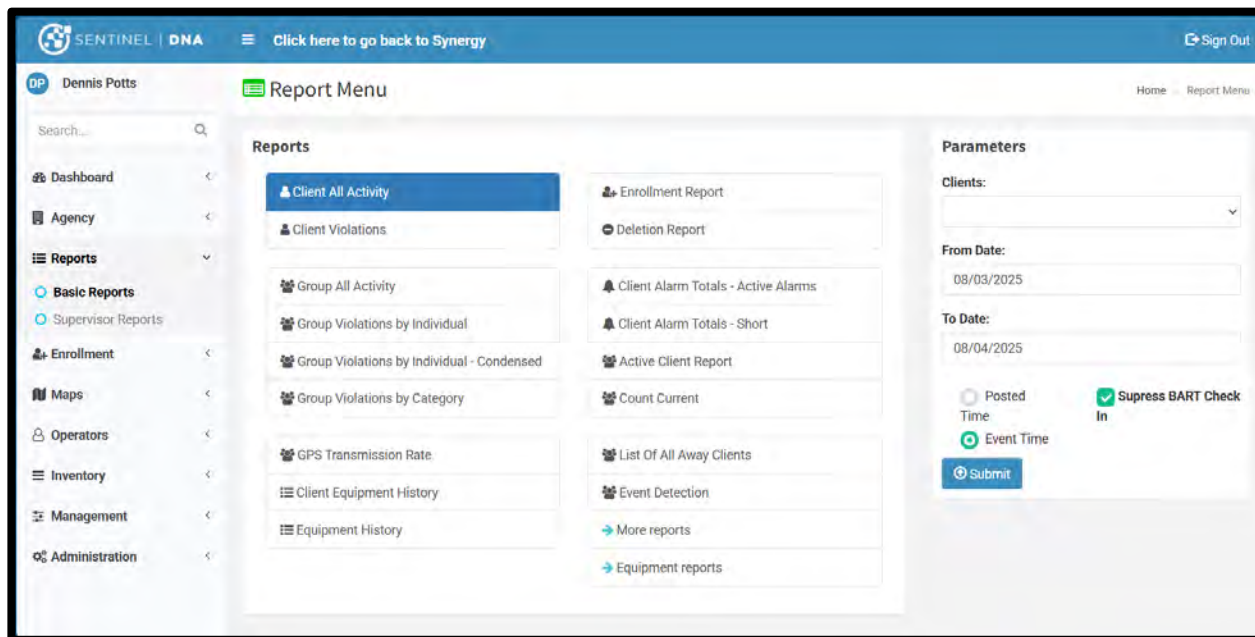
DNA provides additional reporting features for participants who are being monitored via RF Patrol. From the Reports menu and the mapping screen, authorized users can run reports for a single participant or group of people:

- + Alerts showing which actions were taken and whether the notifications were successful
- + Reports showing all events, including alerts/violations and operator comments
- + User Audit Report that shows which users are logging into the monitoring system and for how long

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

DNA REPORT MENU SCREEN



If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

Sentinel's DNA web-based information system is also equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts and violations. Violations can be prioritized to alert immediately or hold for a grace period. The DNA Profile Manager allows for automated notification of alerts as well as optional manual escalation/closed loop communication and sequencing. The

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Profile Manager also differentiates protocol changes within a single alert by time and day of the week. Please refer to the image below for Sentinel's **Notification Procedure** screen within DNA. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

DNA NOTIFICATION PROCEDURE SCREEN

The screenshot shows the 'Profile Viewer' interface for a device named 'Do Not Pass Go Bonding (Version: 1)'. The interface includes a 'Steps' button and a 'Clearing Alarms' status. The main content is divided into two sections: 'Day: Sunday' and 'Day: Monday', each showing a timeline of steps and actions. A 'Back to Profile Manager' button is located in the top right corner.

State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Step 2	Delay	10	Step 3
Step 3	McApp	0	

Instructions: Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue.

Instructions: If no tamper clear, contact officer on duty at the number provided. Close.

Inventory Control Module

—IMPORTANT SENTINEL ADVANTAGE—

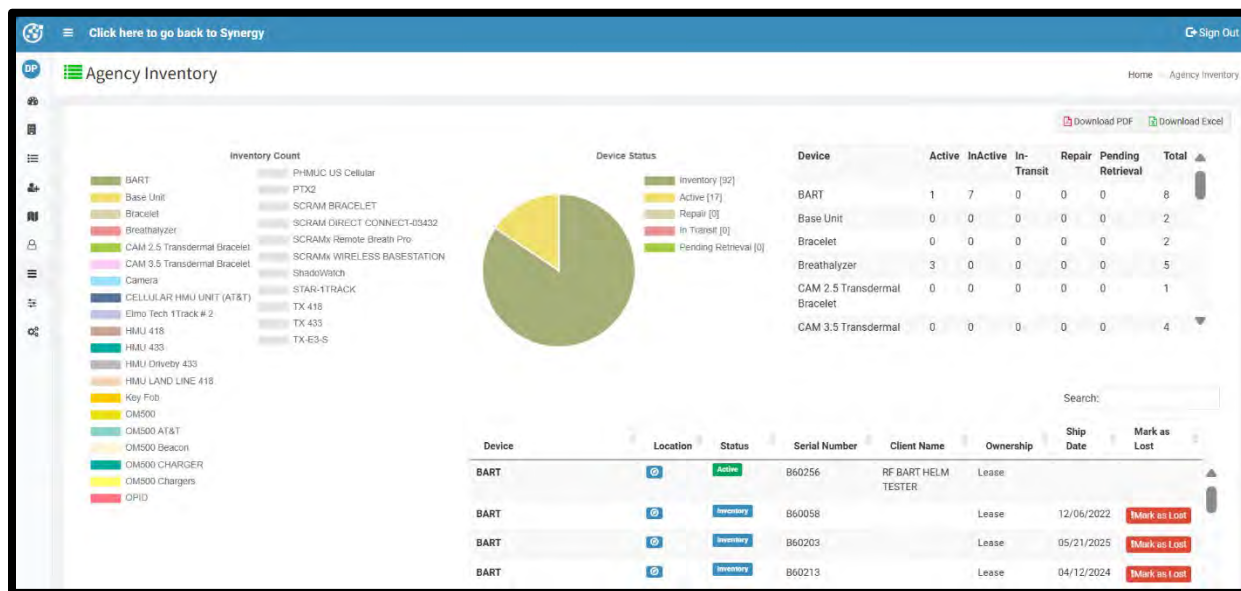
DNA includes an integrated agency Inventory Dashboard providing textual as well as graphical status of all agency equipment inventory and the online capability for users to view status, manage, order, return, track, and transfer equipment. This advanced module will also enable users to request/process/track/manage equipment orders online via DNA. Please refer to the sample DNA agency Inventory Dashboard Screen below.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA AGENCY INVENTORY DASHBOARD



Equipment Retrieval Dashboard

Sentinel has created a unique tool within our DNA monitoring platform to assist agencies with their equipment recovery and inventory control efforts. The **Equipment Retrieval Dashboard** has been designed to provide a visual step-by-step inventory retrieval process for both Sentinel's on-site personnel as well as agency staff. **The Equipment Retrieval Dashboard allows agencies to establish more accurate inventory controls and in turn better manage participant equipment recovery thus reducing equipment loss.**

The Equipment Retrieval Dashboard is located in the Inventory section of our DNA platform. The Dashboard displays a complete list of all devices that were not retrieved from participants upon program completion/violation or who have absconded from the program.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Retrieval Dashboard Home Retrieval Dashboard

[Show Archived Retrievals](#) [Profile Manager](#) [Dashboard Settings](#)

[PDF](#) [Excel](#)

Name	OID	Phone Number	Address	Equipment	Termination Date	Reason for Termination	Last Known Address	Officer / Case Manager
[Name]	ID57995	(808) 7210	Bridgeport, CT06605	Not Retrieved - 30+ Days OmniLink (20560027)	Active		CT 06357, USA	
[Name]	ID57435	(714) 4832	1220 N Simon Cir, Anaheim, CA92806	Not Retrieved - 30+ Days OmniLink (20454852)	Active		Waterbury, CT 06705, USA	SENTINEL TEST /
[Name]	ID57992	(959) 0391	CT06354	Not Retrieved - 30+ Days OmniLink (20426095)	Active		Sprague, CT 06330, USA	
[Name]	ID58022	(475) 3670	K5, East Windsor, CT06088	Not Retrieved - 30+ Days OmniLink (20581862)	Active		Enfield, CT 06082, USA	
[Name]	ID58025	(646) 2525	Bridgeport, CT06610	Not Retrieved - 30+ Days OmniLink (20091750)	Active		Bridgeport, CT 06607, USA	
[Name]	ID57658	(203) 3043	118, West Haven, CT06516	Not Retrieved - 30+ Days OmniLink (20351496)	10/30/2025	Terminated - Violated terms	Hartford, CT 06120, USA	
[Name]	ID58014	(203) 3131	Waterbury, CT06704	Not Retrieved - 30+ Days PHMU (710530) Not Retrieved - 30+ Days PTX (210616)	10/30/2025	Successfully Completed		
[Name]	ID57981	(347) 9942	Stamford, CT06901	Not Retrieved - 30+ Days PHMU (720267) Not Retrieved - 30+ Days PTX	10/30/2025	Terminated - Violated terms		

The Equipment Retrieval Dashboard also allows agencies to create “phases” associated with recovery efforts, which assists in reducing equipment loss by providing a real-time status for each piece of equipment as updated by the officers. These phases are customizable agency-by-agency just like event/alert notification procedures and allow both Sentinel and agency personnel to follow and record step-by-step instructions throughout the recovery process.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Participant Information

Client:

Tran 12345, Ptran - ID5743390

Address:

1220 N Simon Cir, Anaheim, CA 92806

Home Phone:

(714) 209-4832

Cell Phone:

Work Phone:

TimeZone:

PST

Start Date:

04/23/2024

Termination Date:

Active

Reason

Comment

Equipment

OmniLink:

20454852

Mark as Retrieved

Mark as Lost

Location Details

Last GPS Address:

105 Progress Ln, Waterbury, CT 06705, USA

Last GPS Time:

4/24/2024 2:00:35 PM

Contacts

Agency:

CTT

Probation Officer:

5SENTINEL TEST

Officer Cell Phone:

Officer Office phone:

Officer Email:

abyss@sentrak.com

Case Manager:

CM Cell Phone:

CM Office phone:

Case Manager Email:

Phase 1 (Contact)

Comments: Call the participant at all available numbers within the 1st business day of being deleted. NOTE: If the participant does not have valid number; call or email Assigned Officer requesting a valid number.

Phase Results

Spoke to Participant

Spoke to Participant

Spoke to Family/Third Party

Voicemail

Wrong Number/Disconnected

Blocked Call

No Answer

Field Contact

Previous Phase

Next Phase

Export PDF

Export Excel

Phase

No Actions Found!

Comments

Phase Check List

Phase 1

Phase 2

Phase 3

Phase 4

Phase 5

Each Phase or attempt made to recover a piece of equipment is logged within the Equipment Retrieval Dashboard and the Phase Result is added by the person performing the action. This in turn allows the next Phase of the recovery process to be initiated and follow through all other Phases set up by the agency until the device is either recovered or reported to Sentinel as Lost.

If the device is recovered during any point in the recovery process, the officer can go to the Dashboard, select the participant/device and select the "Mark as Retrieved" button to place the device back into the agency's inventory and close out the recovery efforts. Once this has been completed, a report can be generated and exported to PDF detailing the Phases utilized in the recovery effort and notes associated with each attempt.

Equipment - ID854515 Dean, Test

PTX

Retrieved

On 6/8/2022 6:34:19 PM

Serial Number:

208295

Disposition:

Retrieved

Comments

Yet to be Retrieved

Lost

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



OPTIONAL CASE MANAGEMENT MODULE

Unlike other vendors who claim to have a case management system but only have a limited number of fields in their offender monitoring system, Sentinel designed and developed our case management module specifically for these types of programs. Our proprietary web-based information system is designed to be able to handle offender caseloads and all the data and interactions that comprise an offender population. We can track a practically endless amount of data for each offender including:

- + Participant photo
- + Full name and address information (both current and previous residences)
- + Personal information; *i.e.*, Gender, Eye and Hair color, languages spoken, acquaintance information, tattoos or distinguishing body marks (SMTs), aliases
- + Multiple cases (both consecutive and concurrent) present and historical
- + Multiple case numbers
- + Sentence lengths
- + Daily program monitoring fee information
- + Drug Screening
- + Agency information
 - o Court data
 - o Law enforcement or court/probation officer data
 - o Attorney data
- + Employment data
- + Permitted Activities
- + Agency specific tracking data (Booking numbers, "X" numbers, CII numbers)
- + Ability to add additional fields as requested by Agency personnel

In addition to queries, our Active Case Management system can be used to generate the following reports:

- + **Enrollment Notices:** Created when the offender is enrolled in the program.
- + **Completion Notices:** Created when the offender completes the program.
- + **Non-Compliance Reports:** Created for any instance of non-compliance.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **Abscond Reports:** Created for situations when an offender cannot be located due to failure to return to the residence and/or has removed the tracking equipment. Prior to issuing an Abscond, our case managers will have done the necessary research (contacted friends and family, employment sites, and any reasonable alternate contacts to determine the offender's whereabouts).
- + **Termination Reports:** Used when the offender unsuccessfully is removed from the program, including re-arrests or removal by order of the court or other correctional entity.
- + **Status Reports:** Used to report any changes in the offender's status. Also provided as "Progress Reports" when required by Agency personnel.
- + **Schedule Change Reports:** Can be provided to indicate schedule change history.
- + **Court Testimony:** We have program personnel including the Account Manager, as well as corporate personnel that can testify in court.

All our queries and Active Case Management reports can be used to generate comprehensive and all-inclusive reports that can be provided to the Agency at any interval.

More importantly, DNA ensures accurate and consistent posting of payments by utilizing our Automated Payment Application. This application ensures every payment received, whether via credit card, money order, or collections, from the online payment website are appropriately receipted and applied to the participant's account.

The screenshot shows the SENTINEL web application interface. The top navigation bar includes links for Change Group, Select Client, Reports, Report Forms, and Log Out. The left sidebar lists various menu items under 'Development And QA', including Agency, User, Client Info, Client Cases, and Client Payments. The main content area displays the 'Client Debit History' for 'MIA_ID00003 Mark Waugh - Miami Dade Miami Dade'. It includes a table with columns for Date Applied, Debit Type, Comments, and Amount Due. The table shows five entries for 'ELECTRONIC MONITORING' from 2017-05-01 to 2017-05-05, each with an amount of \$7.00. Below the table, there are summary rows for Total Debits (\$35.00), Total Payments (0.00), Balance (\$35.00), and Pay Off Amount (\$933.00). There is also a section for 'Client Debit History' with a checkbox for 'Enable Debit History Range' and date pickers for 'From' (05/01/20) and 'To' (05/05/20), along with an 'Update' button.

Date Applied	Debit Type	Comments	Amount Due
2017-05-05	ELECTRONIC MONITORING		\$7.00
2017-05-04	ELECTRONIC MONITORING		\$7.00
2017-05-03	ELECTRONIC MONITORING		\$7.00
2017-05-02	ELECTRONIC MONITORING		\$7.00
2017-05-01	ELECTRONIC MONITORING		\$7.00
Total Debits			\$35.00
Total Payments			0.00
Balance			\$35.00
Pay Off Amount			\$933.00

MOBILE APPLICATION

The **DNA Mobile Application** is designed for officer use and to streamline feature sets that are available in our full featured DNA website. The abbreviation of certain features and the addition of others in the DNA Mobile App will improve the mobile access experience of our customers using smartphones and tablets. The features of DNA Mobile App were created using valuable input from a panel of supervising officers who routinely work remotely and away from their office. DNA Mobile App facilitates remote supervision like no other and is a valuable tool in the participant supervision process.

Free to our customers, our DNA Mobile App is available for download at the Apple App and Google Play Stores. Compatible with iOS and Android OS, DNA Mobile App utilizes TLS 1.2, AES-256 encryption to ensure all customer and participant data is secure. The DNA Mobile App features:

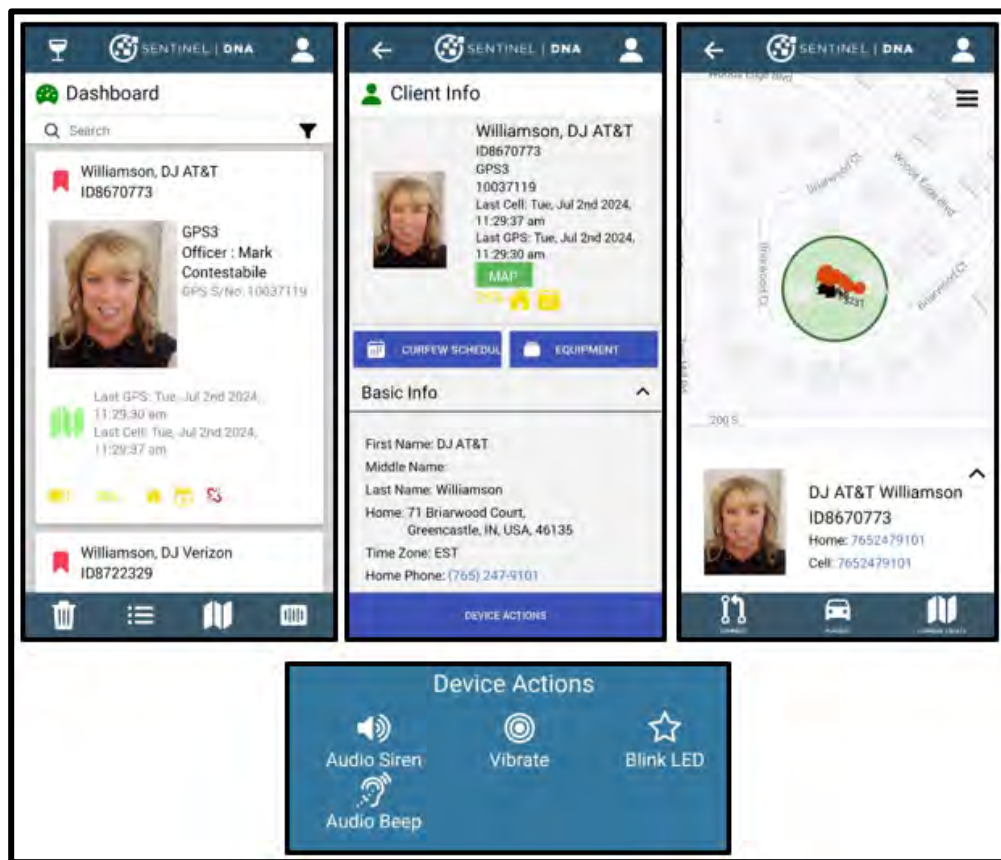
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



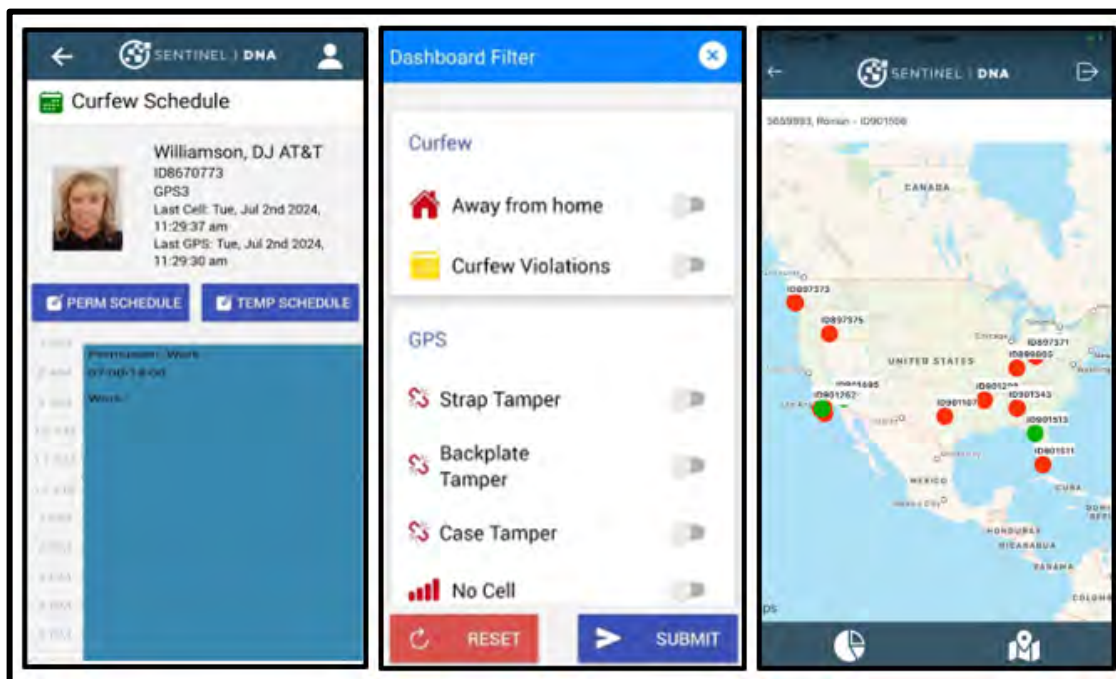
- + **GPS Mapping:** View GPS tracking history, Current Location, and Zones via DNA Mobile.
- + **View and Edit Participant Information:** Modify Participant Name, Device ID, Case Information, Home Address, etc.
- + **Alert Resolution:** View, Respond and Clear Alerts directly from DNA Mobile.
- + **Scheduling:** Quickly update a Participant's Curfew/Home Zone Schedule.
- + **Profile Photograph:** Update participant photos directly through DNA Mobile App.
- + **Travel Directions:** Provides turn-by-turn directions from officer's location to the last known location of the participant or selected address.
- + **Activity Review:** Quickly review all participant activity from GPS and Radio Frequency (RF) devices via DNA Mobile App.
- + **Inventory:** Easily identify inventory availability and status.

The images below display some of the valuable features within our DNA Mobile App.



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



PARTICIPANT COMPANION APP

Sentinel is proud to announce the upcoming release of our latest addition to the SentinelDNA monitoring system and our newest and most innovative smartphone application, the Participant Companion App.

Designed to reduce the number of program alerts and improve communication between the officer/participant while simultaneously improving officer efficiency, the optional Participant Companion App works in conjunction with our SentinelDNA monitoring system and will provide participants with the ability to submit permanent and temporary schedule requests for GPS and/or radio frequency monitoring, upload documents, and "Chat" with their assigned case manager/officer. The Participant Companion App will be available in Q2-2026 for iPhone, Android, and Windows-based smartphone devices for participants designated within their SentinelDNA profiles for app usage. The App can be downloaded onto the Participant's smartphone.

The SentinelDNA monitoring system will provide visual indicators or icons on the Dashboard allowing authorized agency personnel to quickly see pending schedule requests, unread chats and unread document uploads. Authorized users will also be able to click on the icon in order to access the pending items and 1) review, approve, modify and approve, or deny schedule requests; 2) review uploaded documents and save them to the participant's DNA record; and 3) engage in an in-app chat with the participant or multiple participants simultaneously. Agency personnel will also be able to receive real-time notifications via email/text for pending schedule requests and uploaded documents.

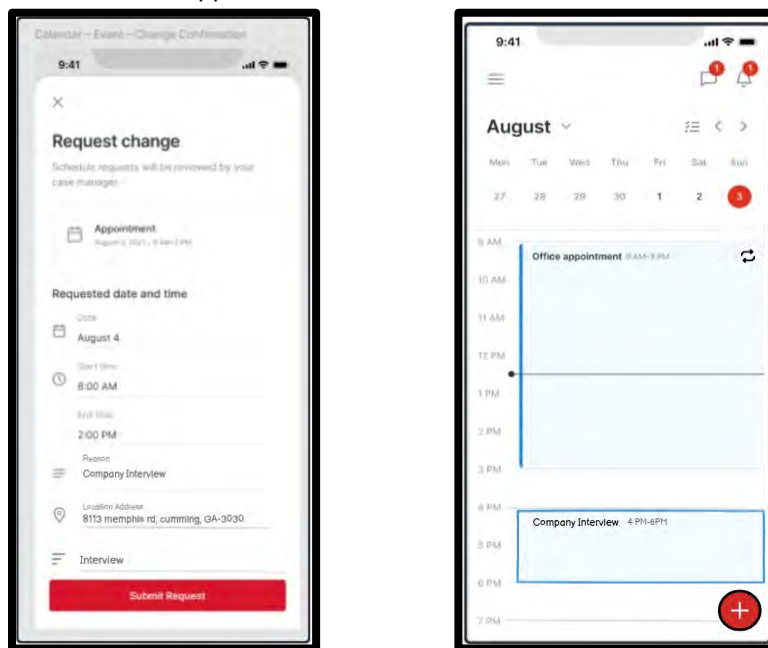
Scheduling Changes Feature. The Companion App will include a feature that allows the participant to request schedule changes directly through the App. The officer will have visibility on this request through DNA and will be able to approve or deny the request with a simple mouse click. If the schedule is approved, it will be automatically delivered to the DNA monitoring system allowing the schedule to change without any further officer interaction. All approvals/denials are communicated back to the participant via the Companion App with all interactions between the officer and the participant captured with DNA.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The Participant Companion App will display the participant's current schedule in the app calendar at all times thereby reducing compliance alerts from the client "forgetting" their schedule. The client will submit schedule requests through the calendar and if approved by their assigned case manager/officer, they will receive notification of the approval along with the new event loading into the calendar. This will allow participants to always have access to their current, approved schedule.



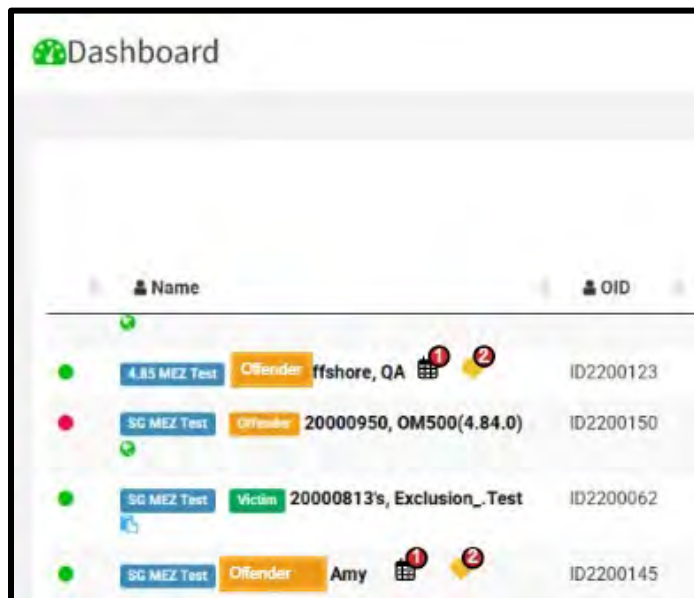
Chat Feature – Participant / Officer Communications. The Companion App also includes the release of a "Chat Feature" that will allow the officer and participant to communicate via chat with all interactions captured and stored in the DNA system for future reference. This feature allows clients to ask quick questions or report issues without waiting for an office visit or playing "phone tag" with the officer, reducing the risk of accidental non-compliance due to miscommunication.

Document Upload Feature. The Companion app will allow the participant to upload required documents, court orders, verification confirmation, etc. directly into the DNA monitoring system via the Companion App. This feature will allow participants to submit required documents to their supervising officer 24/7 without being required to report in person to the office resulting in higher compliance rates by minimizing the time and effort required from the client.

The officer is provided with icons that clearly indicate a client's submitted schedule change request as well as conversations via the chat feature that need to be addressed. The Companion App has been designed to reduce the number of alerts as client schedules are processed immediately upon approval thus reducing the amount of curfew related alerts.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The features associated with the Participant Companion App can be added or removed on a participant-by-participant basis thus allowing officers/case managers control over which features are available to each individual participant.

4. What are the number of settings and general distances of the available range settings of the proposed RF system?

SENTINEL RESPONSE

Sentinel's proposed RF Patrol solution demonstrates a high degree of accuracy though the ability to perform internal range testing and range setting to establish the appropriate preset distance from the home monitoring unit located in the participant's residence and the ankle-worn PTX2 transceiver. Both the RF Patrol PTX2 and the PHMU indicate RF signal strength during range testing enabling the Sentinel on-site program staff and/or agency staff to perform accurate range testing at each installation. The officer/installer can also determine the distance of the range setting in one of multiple distance settings. 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

5. Describe the alerts that can be set up (time, tamper alerts, low battery, etc.). Describe the process for setting system alerts for violations (curfew, tamper). Include the alert intervals and how long it will take for the hardware to communicate with the software. Describe how the technology reduces false tampers and ensures accurate alert notification.

SENTINEL RESPONSE

Sentinel's DNA web-based information system is equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts and violations including curfew, tampers low



battery and all other RF related alerts. Violations can be prioritized to alert immediately or hold for a grace period. The **DNA Profile Manager** allows for automated notification of alerts as well as optional manual escalation/closed loop communication and sequencing. The Profile Manager also differentiates protocol changes within a single alert by time and day of the week. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

The device communicates with the monitoring system at regular, predefined intervals or immediately upon detecting critical events such as tampers. High priority alerts are transmitted in near real time, subject to cellular/landline network availability. Alert notifications are displayed in the monitoring application within seconds of event being received.

RF Patrol has a highly advanced tamper detection scheme. It is a 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. This highly advanced technological design eliminates false "Body Tamper" alerts caused by older generation equipment. The RF Patrol PHMU unit is designed to detect and report multiple types of tampering, including but not limited to power disconnect/reconnect, phone disconnect/reconnect and attempts to open the receiver housing. Additional alerts include:

- + **Battery Alerts for Bracelet and Base Station (Low battery):** Alerts issued when the device battery reaches predefined threshold, allowing proactive intervention before the device powers down.
- + **Power and Motion Alerts for Base Station:** Alerts are triggered when the base station is disconnected from wall power or moved.
- + **Tamper Alerts Bracelet (Strap Tamper) and Base Station (Device Tamper):** Alerts triggered by device strap cuts or case tampering.
- + **Curfew Alerts, Enters, Leaves:** Alerts generated when a monitored individual enters/leaves the range of the PHMU, violates assigned curfew schedules by returning later, or fails to remain within the residence during curfew hours.

6. Describe your customizable reporting. How does the reporting work with court requests and chain of custody requirements for legal purposes.

SENTINEL RESPONSE

SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary



reports or queries.

COURT REQUESTS AND CHAIN OF CUSTODY REQUIREMENTS FOR LEGAL PURPOSES

Sentinel will immediately contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Entity's Data.

Sentinel utilizes a Corporate Custodian of Records in our organization to be the gatekeeper of official subpoenas and Departmental requests for data as it relates to Sentinel's role in the monitoring, supervision, alert notification, and conformance of the delivery of contractually agreed upon service levels.

Sentinel can provide records from DNA system as well as from our Engineering and Quality Assurance Departments in a variety of formats which can be sent via certified mail and/or electronically. Sentinel will include all data requested by the agency.

We understand the required testimony obligations, and Sentinel will provide a subject matter expert to appear in court to discuss equipment, monitoring services, etc., if required. We are fully prepared to provide qualified personnel to provide testimony to describe the functionality, capabilities, and reliability of equipment and reports under oath in a court of law. Upon request of the court and/or in response to a subpoena, Sentinel will provide expert court testimony, either in person or in writing, through witnesses qualified to defend the integrity of our systems and services on behalf of the agency. We also can provide testimony via secure virtual web-based sessions, as needed, which became essential during the COVID pandemic.

We are able to submit the monitoring documentation as supporting evidence when describing the program participant's activities while being monitored. All court testimony is supported by our Custodian of Records who will attest to the validity and accuracy of all monitoring documentation.

When Sentinel receives a records request directly from the court, we produce responsive records in accordance with legal and chain-of-custody requirements. These records are typically accompanied by a **Business Records Affidavit** to establish authenticity and admissibility without the need for live testimony.

The affidavit affirms that:

1. The attached business records were made at or near the time of the events described by, or from information transmitted by, a person with knowledge of those events.
2. The records are kept in the course of Sentinel's regularly conducted business activities.
3. Creating and maintaining these records is a regular practice of Sentinel.

CHAIN OF CUSTODY

To preserve chain of custody for legal purposes:

- + Records are extracted directly from the system of record by authorized personnel.
- + The data is maintained in its original format, without alteration, and any exports are documented.
- + Access, handling, and transmission of records are controlled and traceable to ensure integrity and authenticity from creation through production.

7. Describe your Customer Service, including at least the following:

- a. Hours of operation.



- b. Order procedures (how long to respond to order, delivery time frame). Delivery time after receipt of order? Describe online ordering procedures.
- c. Product request response time (what is kept on hand at office vs ordering products) – inventory on hand.

SENTINEL RESPONSE

Sentinel owns, staffs, and operates both its Primary Monitoring Center and Secondary Monitoring Center. Sentinel owns both the primary National Monitoring Center located at Sentinel's Norco, California, corporate office) and a geographically redundant secondary back-up monitoring center in Atlanta, Georgia. Sentinel's monitoring centers are staffed with trained personnel 24/7/365 and at no time are monitoring services outsourced or subcontracted.

HOURS OF OPERATION

Our monitoring center is staffed 24 hours a day, seven (7) days a week with a supervisor always on duty and live operators cross-trained to support our suite of supervision services and products. This staffing allows Sentinel field staff and agency staff to call and speak with one of our monitoring experts at all times of the day or night. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

Sentinel also provides access to designated help desk staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. This specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

—IMPORTANT SENTINEL ADVANTAGE—

Multiple Warehouse Distribution Centers

To aid our customers, Sentinel a Primary Warehouse located at 1220 North Simon Circle, Unit C, Anaheim, California as well as a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia. With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers. Both locations are open Five (5) days a week during normal business hours from 08:00-17:00 daily.

ORDER PROCEDURES

Sentinel's Help Desk is the point of contact for the ordering of new equipment and the Return Material Authorization (RMA) process. New and return orders are received by the Help Desk via a SentinelDNA monitoring system submission, email, phone call or fax from the customer. Return Material Authorization (RMA) requests submitted to Sentinel are received by the designated Help Desk representative who is responsible for ensuring the order is properly processed and the customer confirmation email is delivered.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



In accordance with Sentinel's Ordering Process, all orders received by 12:30 p.m. (Local Time) are prioritized, processed, and shipped on the day the order is received. Orders received after 12:30 p.m. (Local Time) are processed and scheduled for shipment the next business day.

In accordance with Sentinel's shipping process, orders are prioritized and processed based on the expected Arrival Date at the customer's location. Sentinel staff add new orders received to the Open Orders Report. Once the order is ready to be processed, staff will print and review the Order Details Report for adequacy and prepare the order utilizing one of the shipping methods below. The staff will then change the order status to 'completed' and remove the order from the Open Orders Report once the order has been shipped.

Sentinel's standard shipping method is Ground shipping at no cost to the Participating Entity. For Entities that desire express shipping Sentinel also offers the following shipping methods.

+ Ground Shipping (1-5 business days)	+ 2 nd Day Early AM
+ Express Saver	+ Standard Overnight
+ 3 Day Shipping	+ Priority Overnight
+ 2 nd Day Air	

REQUEST RESPONSE TIME

Sentinel maintains a core inventory of high-demand electronic monitoring equipment at its U.S. distribution centers to support rapid order fulfillment. Requests for items maintained in inventory are typically processed and shipped within one (1) business day of request receipt. Inventory levels are actively managed based on historical usage and forecasted demand to ensure availability and consistent service levels. New devices are received weekly at our warehouse locations and at all times Sentinel maintains available inventory in both the Anaheim and Alpharetta warehouses to ensure timely delivery of customer orders. The volume of weekly deliveries may be increased or decreased based on forecasted needs to ensure warehouse inventory remains available at all times.

Additionally, Sentinel provides equipment for our customers that is stored at the customer's location. This "Shelf Stock" is available to address the day-to-day inventory needs of the program and to allow for ebbs and flows of program size without the need to order/return devices. The amount of Shelf Stock a customer chooses to utilize is determined by program operations, participant enrollments and duration of time on the program. Entities typically carry approximately 10%-15% of shelf stock at any given time.

8. How do you comply with local and state regulations (what type of research do you conduct when working with a new entity?)

SENTINEL RESPONSE

Sentinel strives to remain current and advocate support of legislative initiatives and regulatory initiatives in favor of, never in conflict with, Participating Entity initiatives. Sentinel has been providing electronic monitoring services since 1993 and today operates in more than 40+ states. Since inception, Sentinel has monitored social and political changes that have shaped the criminal justice system and the resulting alternative to incarceration programs where we provide services. Each state and local jurisdiction is subject to laws and regulations that Sentinel complies with both operationally and contractually. With the assistance of Shepperd Mullins, a leading law firm based in California, Sentinel reviews existing and pending legislation and accurately modifies contract documents, participating agreements, amendments, and adjusts operational procedures to remain compliant with local, state and federal regulations. When appropriate, Sentinel supplements our team with attorneys from local jurisdictions to track and monitor legislation that is potentially impactful to the electronic monitoring industry and/or interests of our Entity partners.



When Sentinel receives an inquiry about our products and services or when we approach a government entity and they express a desire to learn about our continuum of products and services, our sales team will research the procurement requirements for that agency as well as research local and/or state statutes that stipulate the use of Cooperative Purchasing Programs. Sentinel has found this to be very effective in our consultative approach as once the agency determines that want to utilize Sentinel products and services, we share with them details on the researched statute and on the cost, time, and convenience the NASPO ValuePoint Cooperative Purchasing Program and the Sentinel Electronic Monitoring Services Contract provides.

Sentinel understands and has experienced the regulatory nuances that must be addressed and complied with both contractually and operationally from county to county and state to state. Examples of Sentinel's regulatory understanding and compliance include the July 1, 2021, California Assembly Bill # 1869 that removed various fees for the cost of administering home detention programs and continuous electronic monitoring. Sentinel tracked, communicated with our government customers, and modified all our impacted contracts to ensure continued compliance. Additionally, we modified our on-site equipment installation and collections services to comply with these new laws. Another example of staying abreast with regulatory requirements includes legislation in the state of South Carolina S.367/H3532 for bond release and requiring electronic monitoring providers to be approved by the South Carolina Law Enforcement Division (SLED). Sentinel has met the SLED Standards and is Certified in the State of South Carolina. Our local staff have completed the required background checks, drug testing and training in accordance with Sentinel and SLED standards. Our record keeping policies are performed in accordance with standards and the required SLED reporting is provided as required. As a SLED certified provider, Sentinel has facilitated information sharing by granting access to our monitoring system to law enforcement agencies.

All of Sentinel's products and services comply with applicable laws. All our products are FCC approved, registered, and certified as required by the cellular networks on which our devices communicate.

Sentinel does not distribute, sell, or otherwise share any information captured during the participant's electronic monitoring period and all records and data remain the sole property of the supervising entity. Moreover, Sentinel complies with all subpoena requests and has an internal Standard Operating Procedure that dictates the steps to be taken to secure evidentiary material and communicate with the legal stakeholders when a subpoena has been served.

Our attorneys along with our senior management team, which have more than 200 years of combined experience in the electronic monitoring industry, will continue to monitor legislative and regulatory changes to ensure ongoing compliance with all applicable laws. Further all future products are developed and certified by the FCC and cellular providers as required to comply with all local, state and federal regulations.

9. Describe the on-boarding process for new Participating Entities.

SENTINEL RESPONSE

SENTINEL ON-BOARDING PROCESS

Sentinel's customer on-boarding is a simplified and strategic process of guiding new Participating Entities through introduction of Sentinel field operations team and the initial planning session that includes discussions on agency setup, review of training curriculum, and discussions on the transition of the products and services to help them achieve their first "win" and value realization with the emphasis aiming to build confidence, improve efficiency, and establish long-term, productive relationships.

Following mutual authorization of the Participating Addendum, Sentinel works with the Participating Entity to finalize an On-Boarding Work Plan and Timeline that includes all known contacts, tasks, deliverables, milestones, and duration estimates for each task and resource loading for the duration of the project. We understand the

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



importance of open and fully transparent operations in the provision of public safety solutions and believe it is essential to the effective operation of any electronic monitoring program. We meet with Participating Entity personnel weekly during the initial implementation stages to review progress, performance, and to identify and resolve any programmatic challenges.

After mobilization, Sentinel continues to meet with the Participating Entity as necessary monthly or quarterly depending on the needs of each Participating Entity. We continue to provide all written reports to the Participating Entity as needed to operate an efficient and effective program including participant activity reports for each program participant and monthly summary reports. In addition, the Sentinel Regional Account Manager continues to always be available through telephone and/or email communications to address concerns or resolve issues with the program.

We work closely with the Participating Entity to ensure all needs, including implementation timeline expectations, are met during implementation and transition. We are highly flexible in our capability for mobilization and adjust our plans and staffing requirements as needed per the decisions mutually agreed in the Initial Project Briefing and Information Session. The following is an example of the elements involved in Sentinel's On-Boarding Process:

On-Boarding Work Plan Milestone	Week 1	Week 2	Week 3	Week 4	Monthly Beginning at Program Start
Initial Project Briefing and Information Session: • Introduction of Sentinel Resource Contacts (Sales, Account Manager, Monitoring Center, Help Desk, Accounting/Billing) • Networking with other Sentinel Participating Entities for sharing Programmatic Policies and Best Practices • Confirmation/Schedule of Initial Order(s), Training and Transition • Agency Notification Profiling, what assistance, if any does the entity need with transferring existing program participants demographic data into Sentinel's Monitoring Application					
Pre-Production Project Evaluation and Analysis					
Design, Development and Testing					
On-site Program Staff Installation and Training					
Equipment Delivery					
Department Training					
Participant Enrollment & Equipment Transition					
Operation and Maintenance					
Assessment of Initial Order Fulfilment					
Ongoing Contract Monitoring and Reporting					



10. Describe the on-boarding process for new Clients. Include any installation information that may apply.

SENTINEL RESPONSE

PARTICIPANT ORIENTATION PROCEDURES

At the first meeting with staff, program clients are provided a full program Orientation. During this Orientation, the rules and regulations of the program are explained, and the client is required to sign the Participant Agreement, which has been customized to meet the needs of the program. Upon completion of the review of the Participant Agreement and based on the activities that the client is allowed to conduct, daily curfew schedules are established clearly detailing when the client can leave their residence for permitted activities.

Staff only allow those activities that are Participating Entity-approved and were established prior to program implementation. In order to verify their whereabouts while away from the residence, clients are instructed on what documentation is required for them to provide at all subsequent compliance appointments. The other tasks at the Orientation include:

- + **Schedule Review** | All daily curfew settings will be reviewed for accuracy and to verify compliance with Participating Entity-approved activities.
- + **Residential Confirmation** | The client will be required to provide proof of his/her residential location. Staff ask for proof of rent payment, monthly home payment note, or official correspondence that verifies the client's place of residence.
- + **Contact Verification** | The client will be asked to provide alternate contact methods. In addition to their personal telephone or cellular numbers, staff attempt to obtain other contact options including contact information for a spouse, friend, or other relative. These additional contact numbers are important when staff are researching an alarm or similar event. All these contact numbers are entered into the proprietary case management system.
- + **Fee Setting** | For those program clients requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule set up with the client.
- + **Next Appointment Setting** | Based on the required reporting schedule of the client, the next face-to-face meeting (Compliance Appointment) will be set at this time. The client will be provided with the appointment information as well as any required documentation that is needed to accompany them in order to ensure compliance.
- + **Question and Answer Support** | If there are any program related questions, the staff member will answer these for the client. If the client ever requests unusual changes such as a modification to their permitted activities, staff will immediately contact the designated Participating Entity personnel to inquire if the change(s) can be approved. Staff will NOT make any changes to the permitted activities or residential status without the prior approval of the designated Participating Entity personnel.

All this information is entered into the client's personal case file in the proprietary case management system, with copies of the statements also kept in the client's physical file at the program office. Participating Entity personnel can have secure access into the case management system to view all case manager-generated reports and notices at any time.

EQUIPMENT INSTALLATION PROCEDURES

Prior to the completion of the Enrollment process (further described below), staff install the required monitoring hardware on the client. As required, staff will perform all necessary steps for "installing" equipment, including enrollment, capturing initial enrollment images for visual compliance-related equipment, etc. The customary equipment installation procedures include:



- + **Preparation of Equipment** | Based on the level of monitoring required, staff will prepare the appropriate equipment type for installation. All equipment is tested by Sentinel's National Warehouse for performance prior to shipment to local field offices.
- + **Data Entry** | Staff will enter the required client information in the monitoring system in order to activate the necessary monitoring or tracking equipment for said client.
- + **Sizing** | If ankle-worn equipment is required for the client, staff will size and fit the ankle-worn device on the client. This is accomplished by adjusting the hypoallergenic ankle strap down to an appropriate size and attaching it to the security holding backplate, which keeps the ankle strap in place.
- + **Installation** | The designated device is secured onto the assembled strap and backplate assembly.
- + **Activation** | The device is activated, and a "good hook-up" is confirmed in the monitoring system. This confirmation is done at the field office to ensure that the client's device is operating as required prior to their departure.
- + **Equipment Guide** | For situations where the client is issued multiple pieces of monitoring equipment, e.g., radio frequency (RF) monitoring and alcohol testing equipment, the staff member will instruct the client how to install the equipment at their residence, in addition to providing them with an instructional flyer illustrating the simple in-home install process if needed.

The Installation process is complete at this time and the monitoring and/or tracking equipment will begin to report all activity and alert information as required. The installation of an ankle device is completed in less than five minutes.

ENROLLMENT PROCEDURES

As the Orientation is being completed, staff create and submit an **Enrollment Notice** to the designated Participating Entity personnel thereby confirming the enrollment of the selected client has been completed. This enrollment notice contains all pertinent client and case information so that the Participating Entity knows all details of the supervision guidelines.

On the Enrollment screen, staff can enter all equipment information, i.e. field monitoring device number, transmitter number, etc. This information is used to properly control Sentinel's internal inventory system for both hardware and accounting purposes. It also allows personnel to quickly ascertain the unit number that a client has been assigned in order to generate monitoring center activity reports.

11. Provide screen shots showing the functionality and user experience of the web-based platform as well as the mobile platform.

SENTINEL RESPONSE

SCREEN IMAGES OF MONITORING SYSTEM SHOWING FUNCTIONALITY AND EASE OF USE

SentinelDNA is Sentinel's in-house proprietary monitoring system designed exclusively for the electronic monitoring industry. The strength of SentinelDNA resides in the system's ability to monitor Radio Frequency, Breath Alcohol, GPS technology and Mobile Applications. The RF Patrol device benefits from all of the SentinelDNA features discussed in the GPS section of this RFP response. For brevity purposes we will outline only the additional items related to RF monitoring and refer the reader back to the Category 1: GPS subsection "**Remaining Category 1: GPS Questions**" (page 86) for more information about the GPS capabilities.

SentinelDNA™ (DNA) is a secure web-based information system that is easily accessible for authorized users 24 hours a day, 7 days a week, 365 days a year. No software components, applications, or client requirements need to be installed by the agency. The SentinelDNA Monitoring System is designed to simplify access and usage across modern browsers on both workstation and laptop computers (Windows, Mac OS X, Linux) and mobile devices (iOS, Android). Additionally, users have the option to view, save, and/or print data and/or reports from the

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



system. This advanced system improves the overall management of program information providing direct access to monitoring data for all authorized agency program personnel.

Designed in-house by Sentinel engineers, DNA can be customized to include all required reports, notification procedures and optional escalation alert sequencing. Moreover, this powerful and easy to use platform will provide the agency with customizable features and benefits not available from other monitoring solutions. DNA makes it easy for officers to access real time information about individual participants or their whole caseload from a secure environment (username and password are required for login). Designed with the needs of end-users in mind, DNA uses a straightforward, intuitive user interface that allows users to efficiently complete all monitoring tasks including:

- + Enroll a participant
- + Create/edit schedules
- + View, create notes
- + Clear events and alerts
- + Locate participants
- + Send custom messages to participant(s)
- + Store and view demographic information
- + Alert processing and advanced triage notification
- + Perform analytics including Point Pattern Analysis and Event Detection
- + Verify and document even contact with participants while in the field
- + Inventory Management including Equipment Recovery Dashboard
- + Perform data management administration
- + Create and edit zones (inclusion and exclusion)
- + Adjust tracking rate plans
- + Review device battery status and charging events
- + Create and print reports
- + Store and view photos and documents
- + Victim assignment and notification
- + Perform audits

Sentinel's monitoring system records all data with a historical transaction record and is stored/archived for retrieval/backup in a database when requested by agency personnel. SentinelDNA Monitoring Application maintains a permanent searchable and reportable record in the form of a: 1) Client Audit Report; and 2) User Audit Report. In addition, all monitoring events and notifications are logged with date and time stamp and are also available for auditable review.

Sentinel's DNA platform offers advanced features and capabilities unavailable in other monitoring and tracking platforms:

- + **Sentinel Designed and Owned:** Engineered, maintained, and monitored exclusively by Sentinel allowing for system personalization as required by the Participating Entity.
- + **Login Authentication:** The system is completely secure and uses state-of-the-art security measures. Sentinel has employed the use of Single Sign-On (SSO) and Multifactor Authentication (MFA) or Two-Factor Authentication (2FA) for our monitoring system that adds an extra layer of protection against phishing attacks and unauthorized access. This step is important for Sentinel and our customers because these changes provide stronger security through centralized authentication and simplifies access across accounts.
- + **Client Dashboard** provides all participant data on one easy-to-read screen. Using straightforward alert icons, the DNA Client Dashboard provides an easy to read at-a-glance interface that allows users to quickly see the status of each participant. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, location information (via mapping), current equipment status, current battery status, as well as zones and curfew schedules.
- + Advanced **automated screen resizing** enables DNA to be accessed by desktops, laptops, tablets and by most leading smartphone browsers without the need to download custom applications.
- + **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 system allows DNA to provide a participant's current location and location history **via Google's map view, satellite/aerial view, bird's eye view, and street view**.



- + **Scheduling** DNA allows users to view and modify all participant curfew schedules and zone schedules as well as view and print monitoring activity reports for all participants. **DNA has the capability to create permanent and temporary schedules and to copy and paste a schedule from one day to the next.** All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.
- + Advanced and extensive **Report Library**, which can be increased at any time at no additional cost. The **Report Library** provides access to all standard system-generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Each data field within the entire information system can be queried to generate necessary report information. **Users have the option to view, save, and/or print data and/or reports from the system.**
- + **Advanced Inventory Control Module** enabling officers/installers 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 equipment orders online via DNA.
- + **DNA Mobile Application** provides officers with mobile access to review participant monitoring data via a smartphone or tablet. Sentinel has developed our DNA Mobile Application for officers to **perform field services and data management work** such as data/schedule changes, equipment changes, de-installations, tracking review, current location requests, etc. from any smartphone or tablet.
- + Optional **Sentinel DNA Case Management Module** that is enabled within our existing DNA monitoring application that handles offender caseloads as well as all the data and interactions that comprise an offender population, including the accurate and consistent posting of client payments.
- + Sentinel has a proven **DNA Application Programming Interface (API)** and is prepared to coordinate with the Participating Entity's Information Technology (IT) to implement an interface between the Participating Entity's systems and Sentinel's DNA application whereby common participant data elements and monitoring data may be automatically pushed/pulled between the two (2) systems, thereby increasing officer efficiency by mitigating the need for duplicate keyed entry into both systems.

Client Dashboard. DNA utilizes an advanced **Client Dashboard** feature that provides authorized agency staff with the flexibility to view all or selected subsets of their entire caseload in near 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 each participant without having to research every record to confirm who is in violation and who is not. From these icons on the dashboard, users can link directly to detailed participant personal information, participant activity, recent events, *location* information (via mapping), *current equipment status*, *current battery status*, as well as *zones* and *schedules*.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT DASHBOARD

Name	OID	Type	Equipment	Compliance	Battery	Profile	Officer
Test Group: Advocate App PT, Carlos	ID8768866	GPS3			47%	Web Only	Dennis Potts
Test Group: Advocate App Vic, Carlos M	ID8768872	VAPP			96%	Web Only	Dennis Potts
Dell, Dee	ID8733643	CM				Web Only	Justin Case
Doe, Jill	ID8718393	VAPP			78%	Web Only	LauraZZZ ZZZDennison
Doe, John	ID8717208	CM				Web Only	LauraZZZ ZZZDennison
HELM Tester, AT&T OM500	ID8719830	GPS3				HELM GPS Testers	Training Department
HELM TESTER, RF BART	ID8748994	RF/BART				Web Only	Marielena Tejeda
HELM Tester, Verizon OM500	ID8693586	GPS3				HELM GPS Testers	Training Department
Jones, David	ID8741640	GPS3			6%	Web Only	LauraZZZ ZZZDennison
Kelso, Jackie (Install)	ID8719098	CM				Web Only	LauraZZZ ZZZDennison
Smurf, Papa	ID8732145	CM				Web Only	Christy Suazo
TCP Test	ID8742997	GPS3				Web Only	LauraZZZ ZZZDennison
TCP Level 3, Christy	ID8758249	GPS3				Christy Tester profile	Vanessa Gonzalez
Wonka, Jenna	ID8735419	CM				Web Only	Training Department

Quick Sorting Feature: Authorized users can refine the information displayed on the dashboard by clicking on one of the columns which then sort the participants based on that parameter. **This allows agency staff to quickly view participants by type of monitoring, by alert, or even by battery percentage.** In addition to sorting the information by column, filter icon buttons (shown below) are displayed at the top right of the dashboard, which allow the user to filter participants based upon the selected status/alert criteria.



For example, by selecting the Tamper icon , only those participants with a Tamper alert are displayed on the dashboard. **This allows agency personnel to quickly review alert information each morning and prioritize contact with participants to better manage their caseload.** Below the sort icons, DNA has a local search option (shown below) to make it easy to refine the dashboard display to specific populations or participants with specific first/last names.



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

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT ACTIVITY SCREEN

HELM Tester, AT&T OM500

Client Personal Info

OID	ID6719830
Reference Number	
Name	HELM Tester, AT&T OM500
Home Ph	(800) 589-6003
Work Ph	
Cell Ph	
Address	1220 N Simon Ct, Anaheim, CA 92805
Timezone	PST

Client Equipment Info

Type	GPS3
Transmitter ID	DT000000
IMEI	10000809
GPS Serial No	10000809
GPS Phone	1
Transmission Rate	15 min(s)

Agency

Name	Sentinel Training Department
Officer	Training Department
Cell Phone	714-726-1114
Work Phone	800-555-6566
Email	csuazo@sentineladvantage.com
24/7 Contact	None
Support Staff	None
Timezone	PST

Clear All Alarms

Client Info

Schedule

Equipment

Location

Zones

GPS Actions

Profile

Activity

Refresh

Add Note

Client Activity

Compliance

Equipment

Battery

Event	Event Time	Received Time
Work Failed To Enter Inclusion Zone	10/21/2025 8:30:10 AM	10/21/2025 8:30:09 AM
Work Late To Enter Inclusion Zone	10/21/2025 8:20:24 AM	10/21/2025 8:20:23 AM
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
Notification sent to monitoring_center@sentineladvantage.com at 10/21/2025 8:03:01 AM		
KMTR Tamper - GPS	10/21/2025 8:02:20 AM	10/21/2025 8:02:47 AM
Backplate Tamper	10/21/2025 8:02:20 AM	10/21/2025 8:02:46 AM

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. **This provides all the important participant information on one screen.**

DNA CLIENT EQUIPMENT STATUS SCREEN

HELM Tester, AT&T OM500

Client Personal Info

OID	ID6719830
Reference Number	
Name	HELM Tester, AT&T OM500
Home Ph	(800) 589-6003
Work Ph	
Cell Ph	
Address	1220 N Simon Ct, Anaheim, CA 92805
Timezone	PST

Client Equipment Info

Type	GPS3
Transmitter ID	DT000000
IMEI	10000809
GPS Serial No	10000809
GPS Phone	1
Transmission Rate	15 min(s)

Agency

Name	Sentinel Training Department
Officer	Training Department
Cell Phone	714-726-1114
Work Phone	800-555-6566
Email	csuazo@sentineladvantage.com
24/7 Contact	None
Support Staff	None
Timezone	PST

Clear All Alarms

Client Info

Schedule

Equipment

Location

Zones

GPS Actions

Profile

Activity

Refresh

Add Note

Client Activity

Compliance

Equipment

Battery

Status	
HOME	Since 3/14/2025 8:03:46 AM
GPS(Strap) Tamper	10/20/2025 6:05:29 PM Clear
BackPlate Tamper	10/20/2025 6:05:29 PM Clear
Potential Shielding	
Potential Sippage	
MEZ Enter	

As illustrated in the Equipment Status screen image above, Officers can quickly view if there is a device issue without wasting time.

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

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Name	OID	Reference Number	Type	Equipment	Compliance
[Redacted]	ID5737143	02972212	RF	[Redacted]	[Redacted]
[Redacted]	ID5806907	02443375	RF	[Redacted]	[Redacted]
102 Victim	ID5803916		GPS3	[Redacted]	[Redacted]
109 Victim	ID5805869		GPS3	[Redacted]	[Redacted]
106 Victim	ID5783386		GPS3	[Redacted]	[Redacted]

Real Time Scheduling, Zones, Authorized users access our DNA Web-Based 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 as well as view and print monitoring activity reports for all participants. All features in DNA are available in near real time, any time, and anywhere via a completely web-based system.

DNA displays participant location information with a date and time stamp for each event. This chronological display is provided on screen as well as in printed report format.

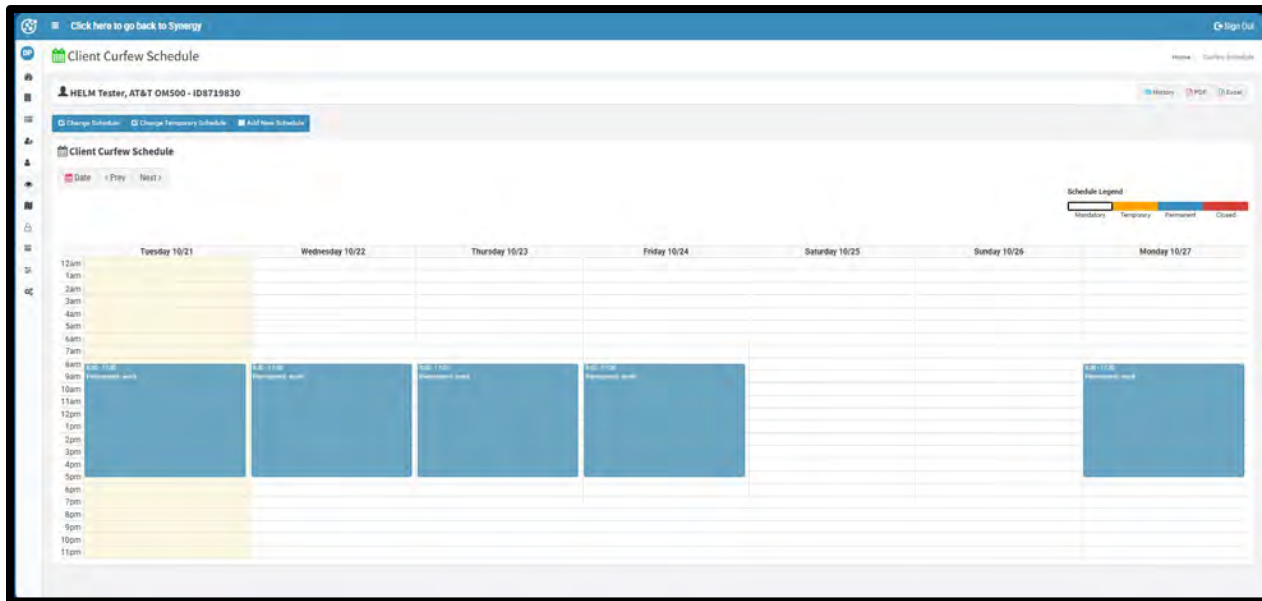
Scheduling. During program enrollments, staff enter curfew/zone schedules and/or inclusion and exclusion zone schedules for each program participant in our DNA web-based system. SentinelDNA schedules allow supervising entities to select specific periods when a participant is required or is not allowed to be within the residence (or range of the RF Patrol device). All leave and enter events are triggered by when the participant leaves the range of his/her PHMU. Each exit from, and entry to, the residence) is reported by the PHMU, and the DNA web-based system automatically compares the activity to the established schedule. This activity verification is continuously performed by DNA, which thereby always ensures the monitoring of each program participant. **DNA also has the capability to create permanent and temporary schedules for both GPS and RF clients and to copy and paste a schedule from one day to the next.**

Request for Proposals for
ELECTRONIC MONITORING

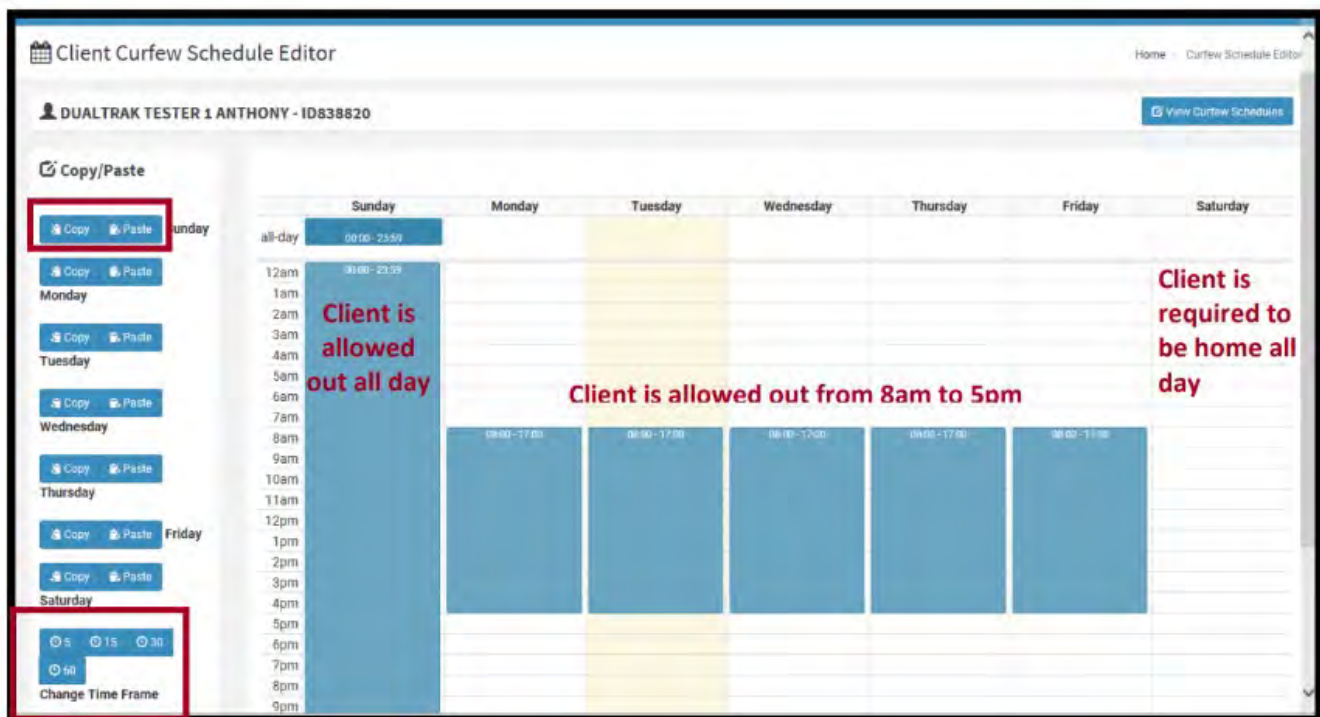
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA CLIENT CURFEW SCHEDULE SCREEN IMAGE



Schedules within DNA define specific time periods when the client is required to be home or is permitted to leave his/her home. If no schedule is assigned to the client, the default setting for each client schedule is "Closed" – meaning the client is not permitted to leave the residence.





Accuracy of RF Reporting. Speed of reporting is typically defined as the round-trip delay of a command and is largely dependent on the underlying radio and cellular network. Under normal operating conditions, this delay is minimal. When RF Patrol is integrated with the DNA platform, the system provides unique capabilities that support both accuracy and reporting speed, including required acknowledgements within DNA to ensure data integrity, while leveraging cellular networks to enable timely transmission and reporting.

An additional design feature that contributes to system accuracy is the inclusion of RF signal level measurement within the PHMU. This capability allows the system to assess the strength of the RF signal, which directly correlates to data reliability and accuracy. Stronger RF signal measurements enable more accurate interpretation of events and environmental conditions, making this a unique feature that enhances overall system accuracy.

Reporting Module and Notification Procedures. SentinelDNA will provide the Participating Entity with access to standard system generated reports that are pre-formatted and available via any Internet-enabled computer or laptop through Sentinel's secure monitoring system. Participating Entities are also able to design and receive customized reports inclusive of desired fields and time frames relevant to their supervision strategies. Any authorized user can view participant activity 24 hours a day, 7 days a week, and authorized users may independently generate reports within the system.. Within our SQL database structure, DNA is infinitely capable of generating reports, eliciting statistical data, and conducting queries/searches for specific information as needed to meet nearly any requirement. Each data field within the entire system can be queried to generate necessary report information.

Users have the option to view, save, and/or print data and/or reports from the system. This advanced system improves overall management of program information providing direct access to monitoring data in the hands of all agency authorized staff. All reports are available for online viewing and printing in Excel, PDF, or Comma-Separated Values (CSV) formats. Reports can be delivered as "Subscriptions" to Participating Entities allowing reports to be executed and delivered at the date and time established by the Participating Entity.

—IMPORTANT SENTINEL ADVANTAGE—

DNA provides additional reporting features for participants who are being monitored via RF Patrol. From the Reports menu and the mapping screen, authorized users can run reports for a single participant or group of people:

- + Alerts showing which actions were taken and whether the notifications were successful
- + Reports showing all events, including alerts/violations and operator comments
- + User Audit Report that shows which users are logging into the monitoring system and for how long

Below we have provided a list of just a few of our standard reports available followed by an image of the Report Menu available within DNA:

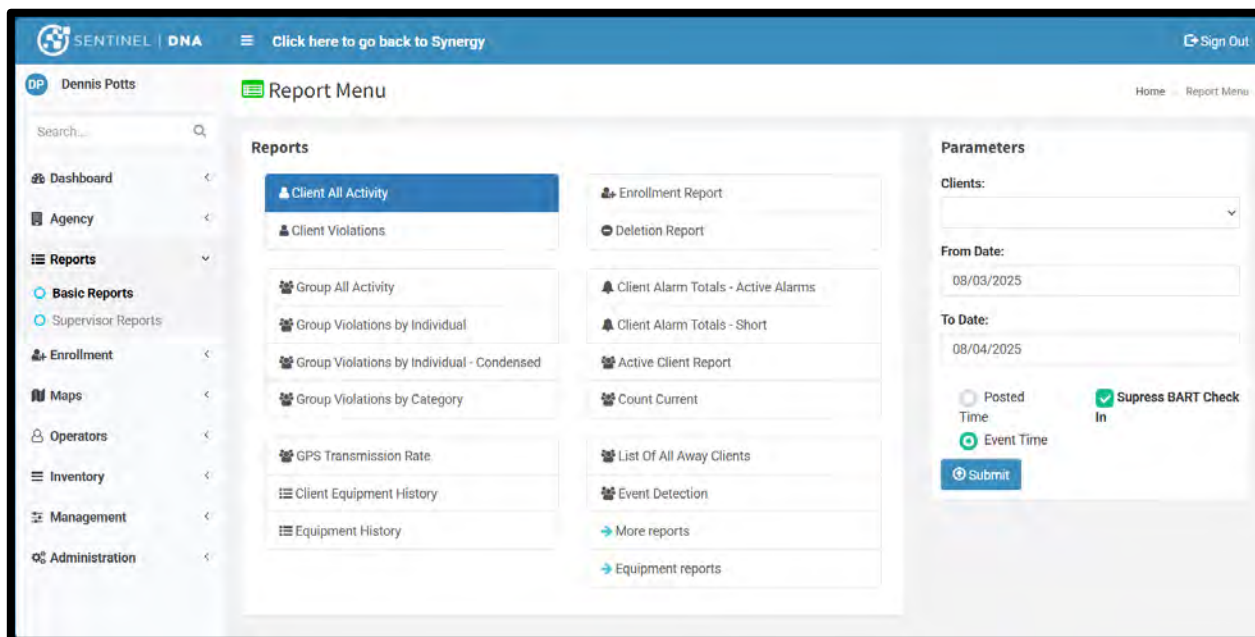
+ Individual All Activity	+ Client Alarm Totals
+ Individual Violations Only	+ Enrollment Report
+ Group All Activity	+ Deletion Report
+ Group Violations by Individual	+ Active Client Report
+ Group Violations by Category	+ Count Current Report
+ Event Detection	+ List of all Away Clients

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA REPORT MENU SCREEN



If the agency requires reporting information that is not currently available through Sentinel's standard reports within our DNA monitoring platform, we will gladly work with the requesting agency to create any necessary reports or queries.

Sentinel's DNA web-based information system is also equipped with the *ability to create custom notification profiles*. Each notification profile is a set of protocols on how to handle alerts and violations. Violations can be prioritized to alert immediately or hold for a grace period. The DNA Profile Manager allows for automated notification of alerts as well as optional manual escalation/closed loop communication and sequencing. The Profile Manager also differentiates protocol changes within a single alert by time and day of the week. Please refer to the image below for Sentinel's **Notification Procedure** screen within DNA. All these procedures are reviewed, discussed and implemented with the assistance of the Regional Account Manager and can be modified/updated at any time as needed.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



DNA NOTIFICATION PROCEDURE SCREEN

Click here to go back to Synergy Sign Out

Profile Viewer

Do Not Pass Go Bonding (Version: 1)
Created on 3/21/2024 8:15:26 PM

Backplate Tamper - GPS11

Steps Clearing Alarms

Day: Sunday
Time: 00:00:00 - 23:59:59

State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Emails: abyss@sentrak.com			
Instruction: Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue.			
Step 2	Delay	10	Step 3
Step 3	McApp	0	
Emails: abyss@sentrak.com			
Instruction: If no tamper clear, contact officer on duty at the number provided. Close.			

Day: Monday
Time: 00:00:00 - 23:59:59

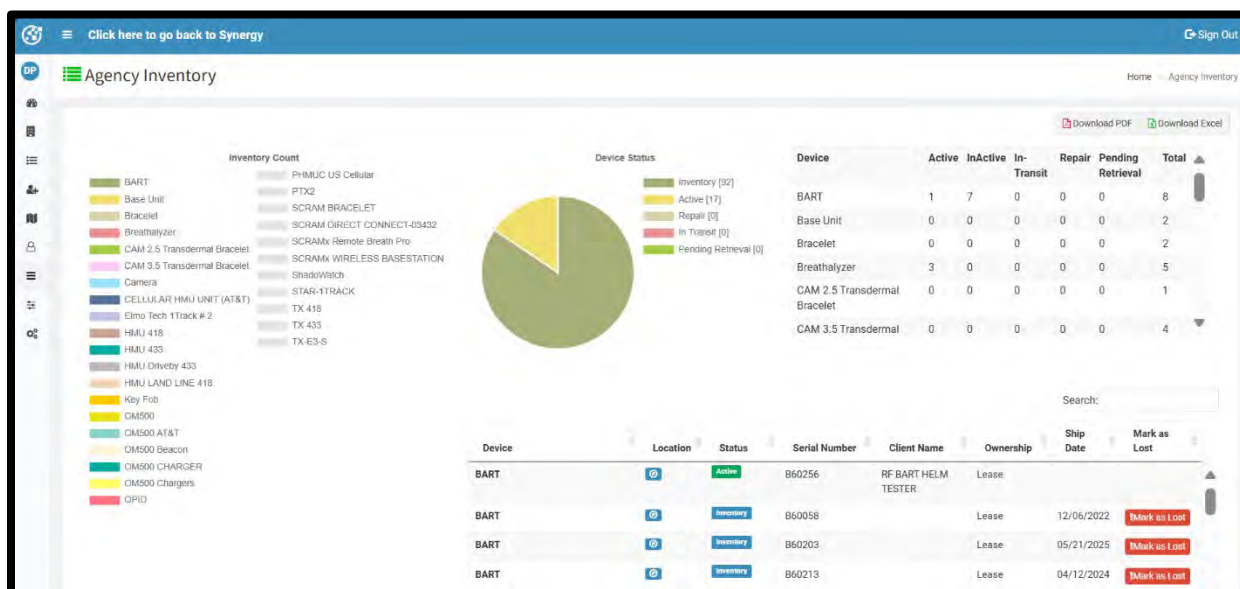
State	Action	State Time	Next State
Step 1	Auto Email and McApp	0	Step 2
Emails: abyss@sentrak.com			
Instruction: Call offender on all available numbers. Obtain statement of current location. Run current locate, click Comment, then click Notify, then Continue.			
Step 2	Delay	10	Step 3
Step 3	McApp	0	
Emails: abyss@sentrak.com			
Instruction: If no tamper clear, contact officer on duty at the number provided. Close.			

Inventory Control Module

—IMPORTANT SENTINEL ADVANTAGE—

DNA includes an integrated agency Inventory Dashboard providing textual as well as graphical status of all agency equipment inventory and the online capability for users to view status, manage, order, return, track, and transfer equipment. This advanced module will also enable users to request/process/track/manage equipment orders online via DNA. Please refer to the sample DNA agency Inventory Dashboard Screen below.

DNA AGENCY INVENTORY DASHBOARD



Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Equipment Retrieval Dashboard

Sentinel has created a unique tool within our DNA monitoring platform to assist agencies with their equipment recovery and inventory control efforts. The **Equipment Retrieval Dashboard** has been designed to provide a visual step-by-step inventory retrieval process for both Sentinel's on-site personnel as well as agency staff. **The Equipment Retrieval Dashboard allows agencies to establish more accurate inventory controls and in turn better manage participant equipment recovery thus reducing equipment loss.**

The Equipment Retrieval Dashboard is located in the Inventory section of our DNA platform. The Dashboard displays a complete list of all devices that were not retrieved from participants upon program completion/violation or who have absconded from the program.

The screenshot shows the 'Retrieval Dashboard' interface. It includes a search bar, navigation buttons for 'Show Archived Retrievals', 'Profile Manager', and 'Dashboard Settings'. Below these are buttons for 'PDF' and 'Excel'. The main table lists equipment with columns for Name, OID, Phone Number, Address, Equipment, Termination Date, Reason for Termination, Last Known Address, and Officer / Case Manager. The table contains several rows of data, some with status indicators like 'Not Retrieved - 30+ Days'.

Name	OID	Phone Number	Address	Equipment	Termination Date	Reason for Termination	Last Known Address	Officer / Case Manager
[Name]	ID57995	(808) 7210	Bridgeport, CT06605	Not Retrieved - 30+ Days OmniLink (20560027)	Active		CT 06357, USA	
[Name]	ID57435	(714) 4832	1220 N Simon Cir, Anaheim, CA92806	Not Retrieved - 30+ Days OmniLink (20454852)	Active		Waterbury, CT 06705, USA	SSENTINEL TEST /
[Name]	ID57992	(959) 0391	CT06354	Not Retrieved - 30+ Days OmniLink (20426095)	Active		Sprague, CT 06330, USA	
[Name]	ID58022	(475) 3670	K5, East Windsor, CT06088	Not Retrieved - 30+ Days OmniLink (20581862)	Active		Enfield, CT 06082, USA	
[Name]	ID58025	(646) 2525	Bridgeport, CT06610	Not Retrieved - 30+ Days OmniLink (20091750)	Active		Bridgeport, CT 06607, USA	
[Name]	ID57658	(203) 3043	118, West Haven, CT06516	Not Retrieved - 30+ Days OmniLink (20351496)	10/30/2025	Terminated - Violated terms	Hartford, CT 06120, USA	
[Name]	ID58014	(203) 3131	Waterbury, CT06704	Not Retrieved - 30+ Days PHMU (710530) Not Retrieved - 30+ Days PTX (210616)	10/30/2025	Successfully Completed		
[Name]	ID57981	(347) 9942	Stamford, CT06901	Not Retrieved - 30+ Days PHMU (720267) Not Retrieved - 30+ Days PTX	10/30/2025	Terminated - Violated terms		

The Equipment Retrieval Dashboard also allows agencies to create “phases” associated with recovery efforts, which assists in reducing equipment loss by providing a real-time status for each piece of equipment as updated by the officers. These phases are customizable agency-by-agency just like event/alert notification procedures and allow both Sentinel and agency personnel to follow and record step-by-step instructions throughout the recovery process.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Participant Information

Client:

Tran 12345, Ptran - ID5743390

Address:

1220 N Simon Cir, Anaheim, CA 92806

Home Phone:

(714) 209-4832

Cell Phone:

Work Phone:

TimeZone:

PST

Start Date:

04/23/2024

Termination Date:

Active

Reason

Comment

Equipment

OmniLink:

20454852

Mark as Retrieved

Mark as Lost

Location Details

Last GPS Address:

105 Progress Ln, Waterbury, CT 06705, USA

Last GPS Time:

4/24/2024 2:00:35 PM

Contacts

Agency:

CTT

Probation Officer:

5SENTINEL TEST

Officer Cell Phone:

Officer Office phone:

Officer Email:

abyss@sentrak.com

Case Manager:

CM Cell Phone:

CM Office phone:

Case Manager Email:

Phase 1 (Contact)

Comments: Call the participant at all available numbers within the 1st business day of being deleted. NOTE: If the participant does not have valid number; call or email Assigned Officer requesting a valid number.

Phase Results

Spoke to Participant

Spoke to Participant

Spoke to Family/Third Party

Voicemail

Wrong Number/Disconnected

Blocked Call

No Answer

Field Contact

Previous Phase

Next Phase

Export PDF

Export Excel

Phase

No Actions Found!

nts

Date

User

Phase Check List

Phase 1

Phase 2

Phase 3

Phase 4

Phase 5

Each Phase or attempt made to recover a piece of equipment is logged within the Equipment Retrieval Dashboard and the Phase Result is added by the person performing the action. This in turn allows the next Phase of the recovery process to be initiated and follow through all other Phases set up by the agency until the device is either recovered or reported to Sentinel as Lost.

If the device is recovered during any point in the recovery process, the officer can go to the Dashboard, select the participant/device and select the "Mark as Retrieved" button to place the device back into the agency's inventory and close out the recovery efforts. Once this has been completed, a report can be generated and exported to PDF detailing the Phases utilized in the recovery effort and notes associated with each attempt.

Equipment - ID854515 Dean, Test

PTX

Retrieved

On 6/8/2022 6:34:19 PM

Serial Number:

208295

Disposition:

Retrieved

Comments

Yet to be Retrieved

Lost

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



OPTIONAL CASE MANAGEMENT MODULE

Unlike other vendors who claim to have a case management system but only have a limited number of fields in their offender monitoring system, Sentinel designed and developed our case management module specifically for these types of programs. Our proprietary web-based information system is designed to be able to handle offender caseloads and all the data and interactions that comprise an offender population. We can track a practically endless amount of data for each offender including:

- + Participant photo
- + Full name and address information (both current and previous residences)
- + Personal information; *i.e.*, Gender, Eye and Hair color, languages spoken, acquaintance information, tattoos or distinguishing body marks (SMTs), aliases
- + Multiple cases (both consecutive and concurrent) present and historical
- + Multiple case numbers
- + Sentence lengths
- + Daily program monitoring fee information
- + Drug Screening
- + Agency information
 - o Court data
 - o Law enforcement or court/probation officer data
 - o Attorney data
- + Employment data
- + Permitted Activities
- + Agency specific tracking data (Booking numbers, "X" numbers, CII numbers)
- + Ability to add additional fields as requested by Agency personnel

In addition to queries, our Active Case Management system can be used to generate the following reports:

- + **Enrollment Notices:** Created when the offender is enrolled in the program.
- + **Completion Notices:** Created when the offender completes the program.
- + **Non-Compliance Reports:** Created for any instance of non-compliance.

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + **Abscond Reports:** Created for situations when an offender cannot be located due to failure to return to the residence and/or has removed the tracking equipment. Prior to issuing an Abscond, our case managers will have done the necessary research (contacted friends and family, employment sites, and any reasonable alternate contacts to determine the offender's whereabouts).
- + **Termination Reports:** Used when the offender unsuccessfully is removed from the program, including re-arrests or removal by order of the court or other correctional entity.
- + **Status Reports:** Used to report any changes in the offender's status. Also provided as "Progress Reports" when required by Agency personnel.
- + **Schedule Change Reports:** Can be provided to indicate schedule change history.
- + **Court Testimony:** We have program personnel including the Account Manager, as well as corporate personnel that can testify in court.

All our queries and Active Case Management reports can be used to generate comprehensive and all-inclusive reports that can be provided to the Agency at any interval.

More importantly, DNA ensures accurate and consistent posting of payments by utilizing our Automated Payment Application. This application ensures every payment received, whether via credit card, money order, or collections, from the online payment website are appropriately receipted and applied to the participant's account.

The screenshot shows the SENTINEL web application interface. The top navigation bar includes links for Change Group, Select Client, Reports, Report Forms, and Log Out. The left sidebar lists various menu items under 'Development And QA', including Agency, User, Client Info, Client Cases, Client Payments, Post Client Payment, One Time Fee, Client Debit History, Client Payment History, and Manage Recurring Fees. The main content area displays the 'Client Debit History' for 'MIA_ID00003 Mark Waugh - Miami Dade Miami Dade'. It includes a table with columns for Date Applied, Debit Type, Comments, and Amount Due. The table shows five entries for 'ELECTRONIC MONITORING' from 2017-05-01 to 2017-05-05, each for \$7.00. Below the table, there are summary rows for Total Debits (\$35.00), Total Payments (0.00), Balance (\$35.00), and Pay Off Amount (\$933.00). There is also a section for 'Client Debit History' with a checkbox for 'Enable Debit History Range' and date pickers for 'From' (05/01/20) and 'To' (05/05/20), with an 'Update' button.

Date Applied	Debit Type	Comments	Amount Due
2017-05-05	ELECTRONIC MONITORING		\$7.00
2017-05-04	ELECTRONIC MONITORING		\$7.00
2017-05-03	ELECTRONIC MONITORING		\$7.00
2017-05-02	ELECTRONIC MONITORING		\$7.00
2017-05-01	ELECTRONIC MONITORING		\$7.00
Total Debits			\$35.00
Total Payments			0.00
Balance			\$35.00
Pay Off Amount			\$933.00

MOBILE APP SCREEN IMAGES

The **DNA Mobile Application** is designed for officer use and to streamline feature sets that are available in our full featured DNA website. The abbreviation of certain features and the addition of others in the DNA Mobile App will improve the mobile access experience of our customers using smartphones and tablets. The features of DNA Mobile App were created using valuable input from a panel of supervising officers who routinely work remotely and away from their office. DNA Mobile App facilitates remote supervision like no other and is a valuable tool in the participant supervision process.

Free to our customers, our DNA Mobile App is available for download at the Apple App and Google Play Stores. Compatible with iOS and Android OS, DNA Mobile App utilizes TLS 1.2, AES-256 encryption to ensure all customer and participant data is secure. The DNA Mobile App features:

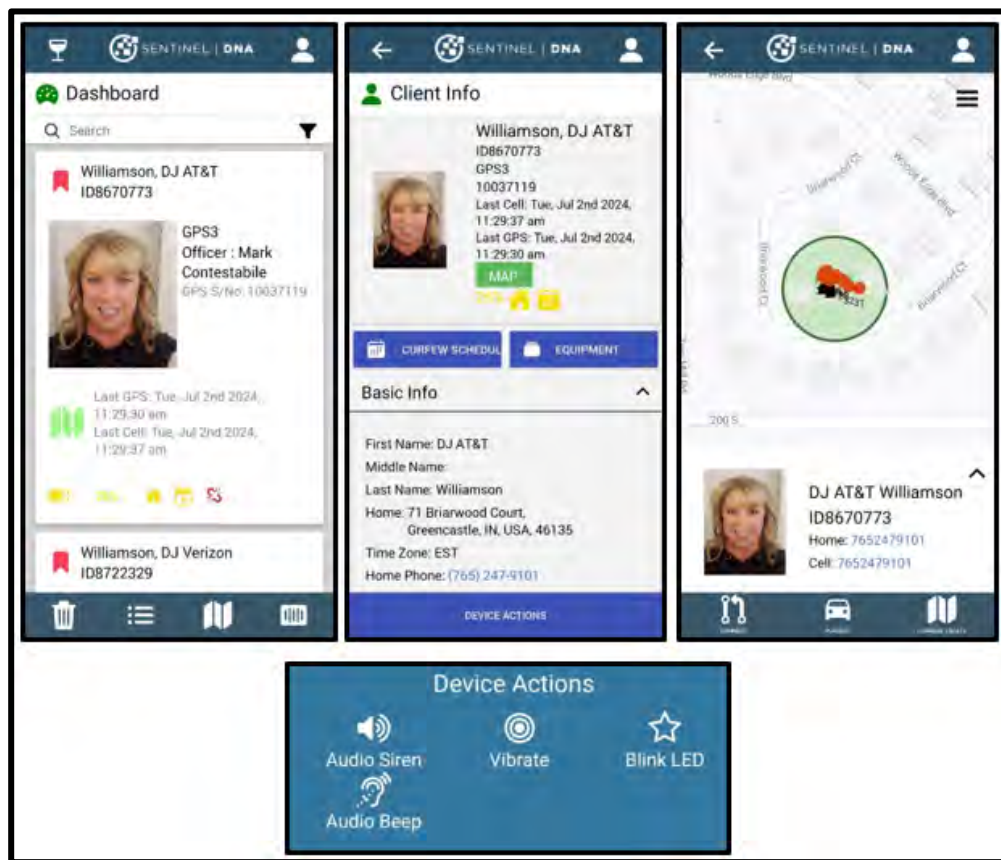
Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



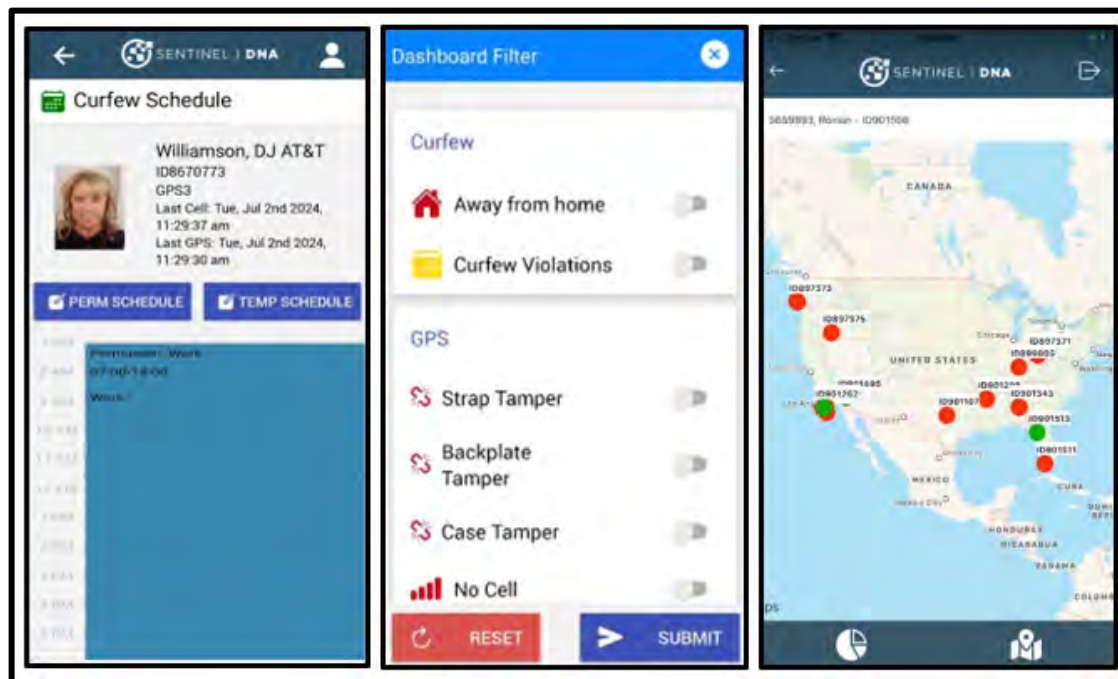
- + **GPS Mapping:** View GPS tracking history, Current Location, and Zones via DNA Mobile.
- + **View and Edit Participant Information:** Modify Participant Name, Device ID, Case Information, Home Address, etc.
- + **Alert Resolution:** View, Respond and Clear Alerts directly from DNA Mobile.
- + **Scheduling:** Quickly update a Participant's Curfew/Home Zone Schedule.
- + **Profile Photograph:** Update participant photos directly through DNA Mobile App.
- + **Travel Directions:** Provides turn-by-turn directions from officer's location to the last known location of the participant or selected address.
- + **Activity Review:** Quickly review all participant activity from GPS and Radio Frequency (RF) devices via DNA Mobile App.
- + **Inventory:** Easily identify inventory availability and status.

The images below display some of the valuable features within our DNA Mobile App.



Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



PARTICIPANT COMPANION APP

Sentinel is proud to announce the upcoming release of our latest addition to the SentinelDNA monitoring system and our newest and most innovative smartphone application, the Participant Companion App.

Designed to reduce the number of program alerts and improve communication between the officer/participant while simultaneously improving officer efficiency, the optional Participant Companion App works in conjunction with our SentinelDNA monitoring system and will provide participants with the ability to submit permanent and temporary schedule requests for GPS and/or radio frequency monitoring, upload documents, and "Chat" with their assigned case manager/officer. The Participant Companion App will be available in Q2-2026 for iPhone, Android, and Windows-based smartphone devices for participants designated within their SentinelDNA profiles for app usage. The App can be downloaded onto the Participant's smartphone.

The SentinelDNA monitoring system will provide visual indicators or icons on the Dashboard allowing authorized agency personnel to quickly see pending schedule requests, unread chats and unread document uploads. Authorized users will also be able to click on the icon in order to access the pending items and 1) review, approve, modify and approve, or deny schedule requests; 2) review uploaded documents and save them to the participant's DNA record; and 3) engage in an in-app chat with the participant or multiple participants simultaneously. Agency personnel will also be able to receive real-time notifications via email/text for pending schedule requests and uploaded documents.

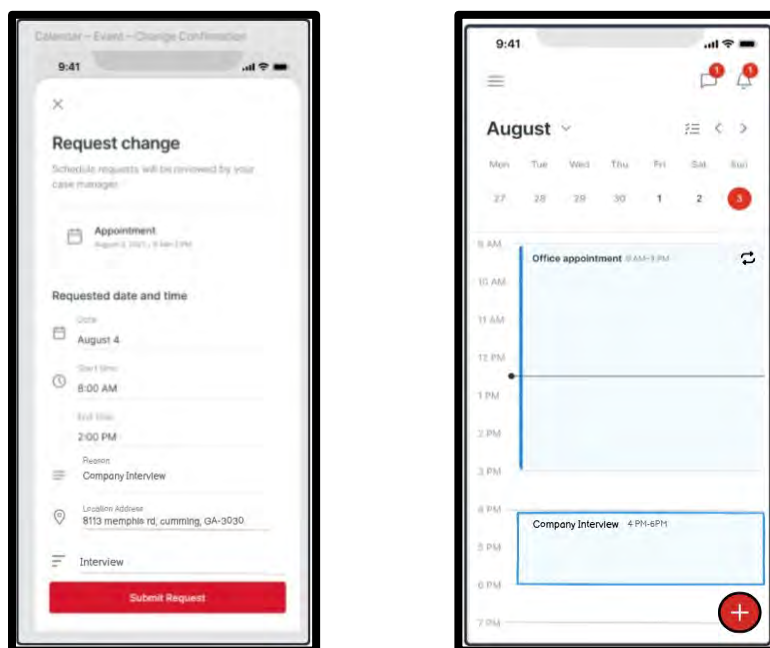
Scheduling Changes Feature. The Companion App will include a feature that allows the participant to request schedule changes directly through the App. The officer will have visibility on this request through DNA and will be able to approve or deny the request with a simple mouse click. If the schedule is approved, it will be automatically delivered to the DNA monitoring system allowing the schedule to change without any further officer interaction. All approvals/denials are communicated back to the participant via the Companion App with all interactions between the officer and the participant captured with DNA.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



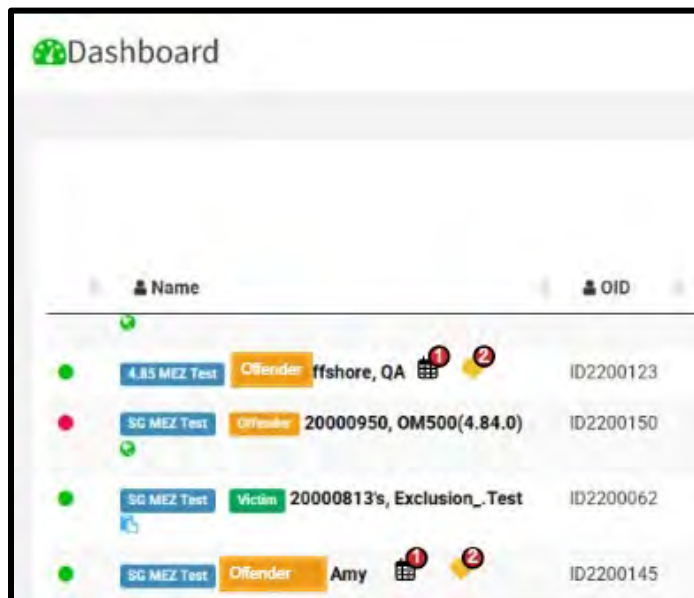
The Participant Companion App will display the participant's current schedule in the app calendar at all times thereby reducing compliance alerts from the client "forgetting" their schedule. The client will submit schedule requests through the calendar and if approved by their assigned case manager/officer, they will receive notification of the approval along with the new event loading into the calendar. This will allow participants to always have access to their current, approved schedule.



Chat Feature – Participant / Officer Communications. The Companion App also includes the release of a "Chat Feature" that will allow the officer and participant to communicate via chat with all interactions captured and stored in the DNA system for future reference. This feature allows clients to ask quick questions or report issues without waiting for an office visit or playing "phone tag" with the officer, reducing the risk of accidental non-compliance due to miscommunication.

Document Upload Feature. The Companion app will allow the participant to upload required documents, court orders, verification confirmation, etc. directly into the DNA monitoring system via the Companion App. This feature will allow participants to submit required documents to their supervising officer 24/7 without being required to report in person to the office resulting in higher compliance rates by minimizing the time and effort required from the client.

The officer is provided with icons that clearly indicate a client's submitted schedule change request as well as conversations via the chat feature that need to be addressed. The Companion App has been designed to reduce the number of alerts as client schedules are processed immediately upon approval thus reducing the amount of curfew related alerts.



The features associated with the Participant Companion App can be added or removed on a participant-by-participant basis thus allowing officers/case managers control over which features are available to each individual participant.

12. Attach the Service Level Agreement for the RF product(s) you are proposing.

SENTINEL RESPONSE

SERVICE LEVEL AGREEMENT

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements ("SLAs"). Please refer to the **Supporting Documentation** (page 340) of this document for Sentinel's Service Level Agreement for the RF products we are proposing.

C. SCOPE OF WORK – CATEGORY 3: ALCOHOL MONITORING

- C. Scope of Work – Category 3: Alcohol Monitoring GPS (Offerors are required to answer all questions if proposing for any Alcohol Monitoring Services. Furthermore, the Offerors shall distinguish which Alcohol Monitoring Services apply to each of the subcategories (CAM/TAC or RAM)
 1. Describe your plan for meeting the Master Agreement Objectives identified in Attachment 02, Scope of Work.

SENTINEL RESPONSE

Below, Sentinel has provided our plan for meeting the Master Agreement Objectives for **Category 3: Alcohol Monitoring**, including CAM/TAC and RAM solutions, identified in **Attachment 02, Scope of Work**.



- VI. Category 3: Alcohol Monitoring.** Offerors are not required to submit for all sub-services under Alcohol Monitoring. To be awarded this category, Offerors must be awarded at least one of the Alcohol Monitoring services listed below.

A. CAM OR TAC

1. CAM Hardware

A. CAM or TAC

1. Hardware Requirements: Continuous Alcohol Monitoring (CAM) that samples an individual client's Transdermal Alcohol Concentration (TAC) and measures for confirmable alcohol consumption on a 24/7 basis.

SENTINEL RESPONSE

Sentinel is offering the SCRAM™ CAM transdermal alcohol monitoring device for the program. The SCRAM CAM transdermal alcohol monitoring system is a comprehensive transdermal ("through the skin") alcohol monitoring system that also incorporates optional house arrest capabilities. The SCRAM CAM device is the most widely used, only scientifically proven and court-validated transdermal alcohol monitoring device available today. The following are highlights on the SCRAM CAM transdermal alcohol monitoring device:



- + Measures the concentration of alcohol in the blood through the skin providing a Transdermal Alcohol Concentration—or TAC—reading;
 - + Battery life of 90 days and requires no involvement or scheduling by the participant, thereby ensuring regular and accurate testing;
 - + Eliminates testing gaps and provides 24/7 coverage, so participants cannot drink around test schedules;
 - + Can withstand changes in temperature and humidity without generating a false positive;
 - + Does not react to other compounds in the environment that create false positives and can consistently distinguish between consumed alcohol and topical or environmental exposure to something containing alcohol;
 - + Does not require a secondary test, such as a breath or blood test administered by a field officer, to confirm a drinking event;
 - + Is independently tested and has peer-reviewed, published studies confirming its reliability;
 - + Includes a comprehensive court support program where the manufacturer will testify in court concerning the technology and specific test results; and
 - + Can prove reliably, in a court of law per the Daubert standard, and has been upheld as valid and reliable by the Daubert, Frye, and FRE 702 and 703 standards of admissibility in every state where it has been used to monitor participants.
- Equipment is at a minimum, shock, water, and tamper resistant.

SENTINEL RESPONSE

The SCRAM CAM bracelet is water and shock resistant, durable, and hypoallergenic. SCRAM CAM is completely water resistant, and all participants are encouraged to shower as frequently and thoroughly as they want.



Additionally, it does not have any exposed water chambers or external features that could freeze in colder temperatures or cause it to stop functioning if it was subject to adverse wearing conditions.

The SCRAM CAM bracelet is equipped with industry-leading, anti-tamper technology that incorporates multiple sensors and accurately detects any tamper attempts. These sensors monitor changes in temperature and any attempt to cut, obstruct, remove, or otherwise defeat the technology. The bracelet's intelligent self-diagnostic capabilities constantly monitor and report its functionality. Any attempts to tamper with the bracelet or its functionality will be immediately detected by the SCRAM CAM system.

- The equipment must monitor ingested alcohol in the human body using court-validated transdermal testing technology and must be able to distinguish between ingested alcohol and environmental exposure to alcohol.

SENTINEL RESPONSE

SCRAM CAM can conclusively distinguish between ingested and environmental alcohol to ensure accurate monitoring due to the unit's (1) controlled, quantifiable sample delivery system, (2) proven electrochemical fuel cell technology, (3) and thorough data analysis and review process by a specially trained team of analysts. This peer-reviewed, scientifically proven, and court-validated confirmation process ensures that only true alcohol consumption events are confirmed.

- The equipment must have a minimum of ~~three (3)~~ two (2) ways to communicate data to the software, such as landline, Ethernet, Wi-Fi, or cellular. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

Sentinel offers landline, cellular/Wi-Fi, and ethernet-based base stations / receivers for use with the SCRAM CAM bracelet. Additionally, the SCRAM CAM unit is the only transdermal unit that can function without the need for a base station or a residential telephone line. Through its Direct Connect computer access, results can be downloaded via laptop or desktop computer by authorized personnel at any location, at any time. Please see below for further details of the base station and Direct Connect device.

- + **SCRAM CAM Bracelet:** The patented SCRAM CAM ankle bracelet transmitter is attached to the participant with a durable tamper alert strap. It is worn 24/7 by the program participant and captures transdermal alcohol readings by sampling the insensible perspiration collected from the air above the skin. For comfort purposes, the ankle strap is hypoallergenic. The bracelet transmits data via a wireless radio frequency (RF) signal to the SCRAM CAM base station. In addition, the SCRAM CAM system has optional house arrest capabilities, allowing it to monitor the wearer's presence or absence within the participant's home.
- + **SCRAM CAM Base Station:** The SCRAM CAM base station is the mechanism by which the data that is collected by the SCRAM CAM bracelet is transmitted for analysis and reporting to the SCRAM Optix system. When the SCRAM CAM bracelet is installed on the participant's ankle, the program participant also receives the SCRAM CAM base station, which plugs into an analog telephone line, usually in the participant's home or place





of work or to an Ethernet connection; a cellular-enabled version is also available for participants who do not have residential telephones or Ethernet connection.

The range between the base station and the bracelet can be set to "Minimum," "Average," or "Maximum" to account for the size of the client's home or other authorized location. These settings are approximately 35, 75, and 150 feet, respectively. The SCRAM CAM base station includes an LED indicator and an audible alarm that can be enabled to alert the client when they are out of range. The SCRAM CAM base station can hold up to a month's worth of data (about 7500 messages). This equates to about 48 tests per day, or 1,440 tests per month. All messages are time-stamped and stored in its non-volatile memory, so that the messages are never lost.

The SCRAM CAM base station is optimized to communicate by standard telephone line or the Internet using the Ethernet port, as well as Wi-Fi and cellular connectivity. The bracelet communicates all alerts with the base station when in range, which then sends all available data to the monitoring system. At a pre-scheduled time(s) each day, the SCRAM CAM bracelet "communicates" with the base station, which then retrieves all available data from the bracelet and sends it for review. The base station also downloads monitoring and reporting schedules to the bracelet. Additionally, the SCRAM CAM base station is available with **Ethernet connectivity** to allow the unit to communicate over the internet using the participant's home modem. The Ethernet port at the back of the base station connects to almost all modems, regardless of internet service provider. Ethernet connectivity is a modern alternative to landline communication.

- + **SCRAM CAM Direct Connect:** In cases where a program participant may be required to report to agency personnel on a weekly basis, he or she can come into the supervising authority's office to have data that has been stored in the bracelet downloaded via the SCRAM CAM Direct Connect device. The compact Direct Connect device is slipped over the participant's bracelet (while worn) and attached by USB cable to an internet-enabled computer. The stored information is then transmitted from the SCRAM CAM bracelet directly for review without the need for a base station.

- The equipment must have the ability to determine equipment's proximity to the body of the client being monitored, including detection of obstructions and changes in body temperature.

SENTINEL RESPONSE

The SCRAM CAM bracelet's advanced anti-tamper technology includes multiple sensors designed to detect any attempts to defeat or interfere with the device's monitoring capabilities. Specifically, the bracelet is capable of identifying proximity tampering—situations where foreign objects or barriers are placed between the bracelet and the skin to obstruct its function. These sensors continuously monitor for changes in temperature, interruptions in skin contact, and any attempts to cut, block, or remove the bracelet. If the bracelet loses proximity to the skin or detects any obstruction, its intelligent self-diagnostic system instantly flags the event and reports it to the SCRAM CAM system for immediate review. This ensures that proximity tampering, along with other forms of interference, are reliably detected and addressed to maintain the integrity of alcohol monitoring.

- The equipment must utilize a commercially available and proven fuel cell technology (e.g. Dräger) that tests a controlled sample of perspiration of the client.

SENTINEL RESPONSE

The electrochemical fuel cell, which is the heart of the SCRAM CAM bracelet, has been proven through decades of research and experience and is considered the gold standard in alcohol testing applications. This is the same



type of fuel cell used in evidential breath testing equipment and interlock devices, and it is comprised of extremely sensitive and ethanol-specific alcohol sensors.

- The technology must have single source admissibility, meaning the CAM device does not require agency staff to issue a secondary testing methodology to verify consumption on an alcohol alert.

SENTINEL RESPONSE

SCRAM CAM is single source admissible, which means it never requires a secondary test, such as a breath or blood test, to confirm a drinking event. It can conclusively distinguish between ingested and environmental alcohol to ensure accurate monitoring. This is possible due to the following reasons:

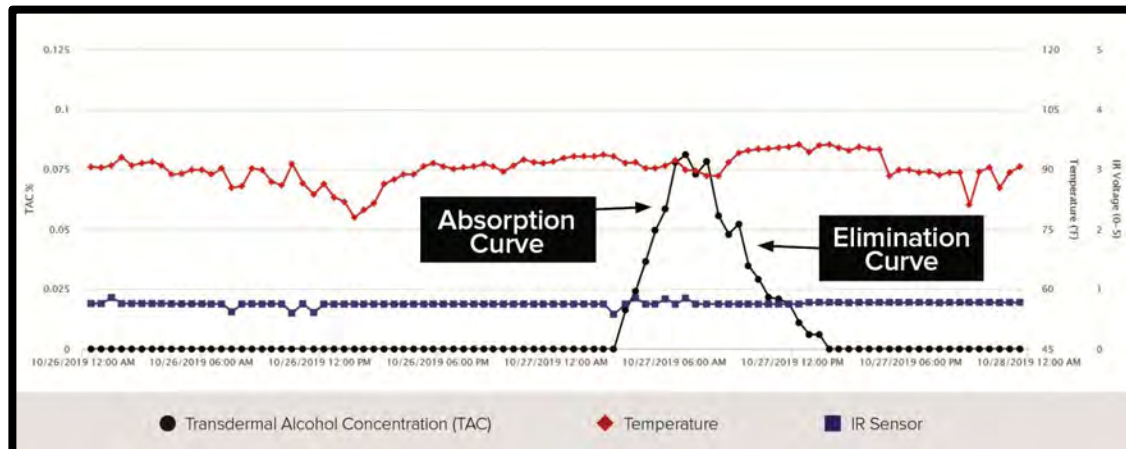
- + **Controlled, Quantifiable Sample Delivery System.** SCRAM CAM is the only CAM device on the market that uses a controlled, quantifiable sampling method—collecting every second—to create a measured sample every 30 minutes. This is the same proven type of sample delivery system used in evidential breath testing equipment that has been the standard in law enforcement for decades. Without this sampling method, a device is susceptible to environmental factors causing false positives and/or may require a secondary test. By combining this system with “contaminant isolation”, SCRAM CAM can distinguish between environmental and ingested alcohol.

The sample delivery method results in a quantifiable Transdermal Alcohol Concentration (TAC) curve, with specific alcohol absorption and elimination rates. The contaminant isolation method allows SCRAM CAM to measure the level of environmental or ambient alcohol prior to each transdermal alcohol measurement, indicating if a test has been contaminated. When combined, these approaches ensure results of the highest confidence with the lowest false positive rate possible.

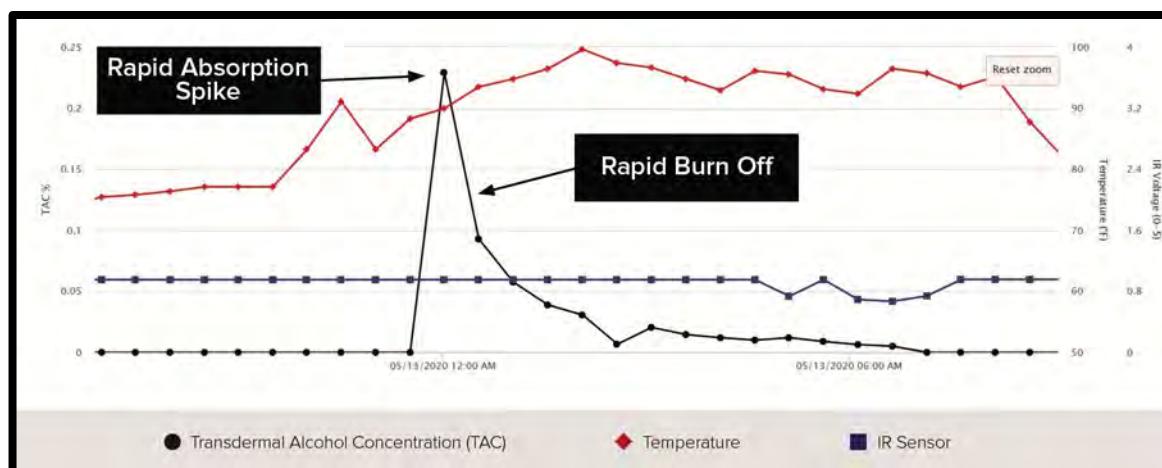
- + **Proven Electrochemical Fuel Cell Technology.** The electrochemical fuel cell, which is the heart of the SCRAM CAM bracelet, has been proven through decades of research and experience and is considered the gold standard in alcohol testing applications. This is the same type of fuel cell used in evidential breath testing equipment and interlock devices, and it is comprised of extremely sensitive and ethanol-specific alcohol sensors.
- + **Thorough Data Analysis and Review Process.** All data received from the SCRAM CAM bracelet is subjected to a rigorous, scientific alcohol detection analysis. This review process, supervised by a specially trained team of analysts, looks at key data (such as alcohol absorption and elimination rates) of the TAC curve. This peer-reviewed, scientifically proven, and court-validated confirmation process ensures that only true alcohol consumption events are confirmed.
 - o **Confirmed Alcohol Consumption.** SCRAM CAM readings and analysis are based on the well-documented and scientifically proven metabolism rate for consumed alcohol. Data from a drinking event shows a gradual increase in alcohol levels over time, achieves a maximum TAC, and then slowly burns off to create a well-defined alcohol curve. In the following graph, TAC is represented by the black line. Tamper detections, in the form of an infrared (IR) sensor (represented by the blue line) and temperature reading (represented by the red line) appear on the graph along with the TAC readings.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- o **Environmental Alcohol Detection.** The graph below depicts a client coming into contact with an environmental alcohol source (like lotion, perfume, etc.). It shows a distinct and dramatic jump in the absorption side of the alcohol curve, followed by a rapid dissipation of the alcohol, unlike the graph of an actual drinking event. It shows absorption and burn-off rates outside of the tested, proven rates that the body can absorb and metabolize for consumed alcohol. In addition, before every 30-minute measurement, SCRAM CAM tests the ambient air around the device to determine if environmental alcohol is present.



- Device must have demonstrated a history ~~of outside research or published studies by an entity other than the manufacturer itself~~, highlighting the validity of the product or establishing general acceptance in the ~~scientific electronic monitoring~~ community. ~~(References for outside research studies published on the proposed solution must be provided upon request).~~
[Edited per Amendment # 3, Scope of Work_ Revised 2.6.26~2]

SENTINEL RESPONSE

The OEM of the proposed CAM device, SCRAM Systems, has a well-documented history highlighting the validity of the SCRAM device. One such study was performed by the U.S. Department of Transportation Highway Traffic Safety Administration. This comparative study reviewed and evaluated the use of SCRAM in conjunction with recidivism rates and characteristics. This study was published in April 2015 and highlights not only the benefits



associated with the SCRAM transdermal alcohol testing device but also provides additional information and references case studies within the states of Wisconsin and Nebraska. Additionally, an article was published by Sheila M. Alessi, Nancy P. Barnett, and Nancy M. Petry that outlines the experiences with SCRAM alcohol monitoring technology in 100 alcohol treatment outpatients.

- Optional: The CAM device should have the ability to perform optional RF (Radio Frequency) home curfew monitoring in addition to continuous alcohol monitoring when needed.

SENTINEL RESPONSE

The SCRAM CAM bracelet can be used as CAM-only or combined with integrated radio frequency (RF) house arrest for location monitoring. Authorized program users can easily enable the house arrest feature through the monitoring solution at any point during a client's supervision period without the need to change equipment. The SCRAM CAM base station provides house arrest / curfew monitoring as well the mechanism by which the data that is collected by the SCRAM CAM bracelet is transmitted for analysis and reporting to the monitoring system.

The SCRAM Base Station is optimized to communicate by standard telephone line or the Internet using the Ethernet port, as well as Wi-Fi and cellular connectivity. The bracelet communicates all alerts with the base station when in range, which then sends all available data to the monitoring system. The range between the base station and the bracelet can be set to "Minimum," "Average," or "Maximum" to account for the size of the client's home or other authorized location. These settings are approximately 35, 75, and 150 feet respectively. The SCRAM CAM base station includes an LED indicator and an audible alarm that can be enabled to alert the client when they are out of range.

If monitoring via landline and the base station is disconnected and reconnected to an unauthorized telephone line, the SCRAM CAM base station will generate an alert, as well as indicate the number from which the base station is calling. If monitoring wirelessly, an alert will be generated if the base station is moved.

The SCRAM CAM base station is powered by the client's home AC power outlet. If it becomes unplugged or loses power, it will switch to the backup battery and an "AC Power Loss" message will be called into the monitoring system. The backup battery will function for up to 48 hours during a power outage with a fully charged battery. When electrical power is restored, it will switch back to main power, and an "AC Power Restore" message will be called into the software. If telephone service is lost, the base station will log a "Telephone Loss" message. When telephone service is restored, the base station will log a "Telephone Restore" message and communicate both messages to the monitoring system. The SCRAM CAM base station can hold up to a month's worth of data (approximately 7,500 messages), which equates to about 48 tests per day or 1,440 tests per month. All messages are time-stamped and stored in the unit's non-volatile memory. All alerts will be reported to the contracting agency per pre-defined procedures.

2. CAM Software

2. Software Requirements: The systems must collect, transfer, and store historical client information (alcohol consumption and tamper information) 24x7 days per year in an encrypted manner and retrievable upon request.

SENTINEL RESPONSE

SCRAM Optix creates an integrated, dynamic user experience that allows officers to manage their entire SCRAM CAM and SCRAM Remote Breath Pro caseload with a single login. Through this secure platform, officers can enroll clients, manage alerts, adjust device settings, enter and edit schedules, select notification methods or parameters, manage inventory, access full caseload details, and configure a variety of reports. The software is



available 24/7 via any Internet-enabled device with a mobile-adaptive design that allows officers to work by desktop, tablet, or smartphone. Access to Optix is encrypted and protected at all times.

SCRAM Optix is the central information hub where SCRAM CAM and SCRAM Remote Breath Pro client data is collected, analyzed, and maintained in a secure, central location. This web-based application not only houses all client data but allows courts and supervising agencies to access and manage their data from any web-based browser. In addition, the software provides a wide range of reports and graphs—from a snapshot of a single event to a comprehensive view of a client's behavior over time. Authorized personnel can do the following through the web-based software application:

- + View information about the client, including—but not limited to—personal information, current electronic monitoring data, historical electronic monitoring data, violation statuses, notification settings, and reports.
- + Enroll/edit/remove clients without calling the monitoring center.
- + Create, edit, delete, and apply monitoring parameters (such as daily/weekly schedules) for clients when using RF/House Arrest monitoring.
- + Determine which violations/events must trigger notifications and by what means the notifications must be sent to agency personnel.
- + Set up notification to be sent to agency personnel.
- + Customize and tailor reporting that best suits their needs, further helping to reduce officer workload.

- Web-based platforms accessible via desktop, tablet, and mobile devices.

SENTINEL RESPONSE

SCRAM Systems provides a comprehensive, secure, and fully integrated supervision technology platform designed to support alcohol monitoring, location monitoring, and client engagement through both web-based applications, such as desktops and tablets, and smartphone-based applications / mobile devices. These applications operate together to provide real-time data visibility, improve officer efficiency, and ensure the accuracy and timeliness of monitoring information.

- Secure login with multi-factor authentication.

SENTINEL RESPONSE

SCRAM Optix is a secure, web-based platform that requires authenticated user access. The system supports secure login protocols and role-based authentication to ensure that only authorized personnel can access system data. Access to Optix is encrypted and protected at all times, and agencies may enable additional authentication controls based on internal policy.

- Automated notifications and alerts (via SMS, email, or in-platform) for violations such as zone breaches, tampering, missed tests, or low battery. Including but not limited to:
 - o high atmosphere alcohol
 - o alcohol detected report,
 - o dual alerts (both high atmosphere and alcohol detected),
 - o below-temperature conditions,



- o and prolonged high atmosphere readings

SENTINEL RESPONSE

SCRAM CAM provides a comprehensive, automated alerting system that supports email, text/SMS, and in-platform notifications; notifications will also be delivered via the Dail Action Plan. The SCRAM Optix monitoring platform automatically generates alerts for all CAM-specific violations and device conditions. All alerts are stored within the platform and are date- and time- timestamped for complete auditability. Before alerts are sent, each CAM-specific violation is reviewed and validated by trained analysts to ensure accuracy. The system will provide the following alcohol-related alerts:

- + **High Atmosphere Alcohol:** The SCRAM CAM device measures ambient alcohol around the bracelet before every scheduled test. Significant or unusual atmospheric alcohol readings trigger an alert within the monitoring platform, supporting the identification of environmental interference.
- + **Alcohol Detected (Confirmed Drinking Event):** SCRAM CAM conducts continuous transdermal testing and analyzes alcohol absorption and elimination patterns to detect and confirm alcohol consumption. When results align with a true drinking event, the system issues an automated alcohol-detected alert.
- + **Dual Alerts (High Atmosphere + Alcohol Detected):** Because SCRAM CAM measures both environmental alcohol and transdermal alcohol concentration independently, the system can simultaneously identify both conditions. When this occurs, separate alerts are generated to indicate the presence of environmental alcohol and a confirmed drinking event.
- + **Tamper-Related Alerts:** The SCRAM CAM bracelet includes multiple anti-tamper sensors that detect temperature changes, loss of skin contact, obstructions, removal attempts, or any action intended to interfere with the device. Any tamper event is immediately flagged and transmitted as an alert to supervising authorities.
- + **Communication Alerts:** Communication failures—such as loss of power, loss of telephone or network service, or the device being out of range—generate system-level alerts. These alerts are automatically transmitted to the monitoring system, ensuring supervising officers are promptly informed of any disruption in testing or data transmission.
- + **Low Battery Alerts:** SCRAM CAM provides advance notification of low battery status approximately seven (7) days before the expected end of battery life to ensure that staff have sufficient time to replace the battery before monitoring is interrupted.
- + **Below-Temperature or Abnormal Temperature Conditions:** Temperature sensors continuously verify proper skin contact. If the device records temperatures outside the expected range, an alert is generated, as these conditions may indicate a removal or tamper attempt.
- + **Prolonged High Atmosphere Readings:** If sustained environmental alcohol readings occur over multiple sampling intervals, the system recognizes this pattern as potentially significant and accordingly generates alerts; these alerts help differentiate normal, short-term environmental exposure from conditions that may affect monitoring integrity.

- Reporting capabilities with customizable fields, exportable in PDF, Excel, and CSV formats.

SENTINEL RESPONSE

SCRAM Optix provides a comprehensive reporting suite with customizable fields for both client-level and program-level reporting. Reports can be exported in multiple formats, including PDF and Excel, and support structured data exports suitable for CSV-based workflows. Reporting options include summary reports, detailed event histories, compliance analytics, and program-wide data views, all configurable to meet agency or court requirements.



- Integration options with existing case management systems through APIs.

SENTINEL RESPONSE

SCRAM Optix includes built in API and integration middleware capabilities that allow seamless data exchange with third party case management systems. Agencies may automate client record updates, receive monitoring data, sync alerts, and streamline workflows without duplicate data entry thereby ensuring compatibility with modern court, probation, and corrections case management environments.

- Audit trail and data retention in compliance with CJIS security requirements.

SENTINEL RESPONSE

SCRAM Optix maintains a complete and immutable audit trail for all device events, alerts, user actions, and monitoring results. Every action is time-stamped and retained according to strict data-integrity controls. The system's security and data-management framework is aligned with criminal-justice security expectations, providing full traceability for evidentiary purposes and long-term data retention requirements.

- Role-based access controls for administrators, supervisors, and officers. The system must provide security features, which must prevent unauthorized individuals from accessing any information held by the Contractor. Secure access to the system must be always maintained.

SENTINEL RESPONSE

SCRAM Optix provides configurable role-based access controls allowing agencies to assign permissions based on job function – including administrator, supervisor, officer, and read-only tiers. Each role determines access to client information, alert management, reporting, device controls, and administrative configurations. System safeguards ensure unauthorized individuals cannot access any data, and secure access is maintained at all times through controlled permissions, encrypted communication, and user management protocols.

- The system must provide the capability for Participating Entity to download data and reports from the database, through secure internet access.

SENTINEL RESPONSE

The SCRAM Optix system provides secure internet access for the Participating Entity to download data and reports from the database.

- The bracelet must be capable of storing at least 30 days of time stamped client data regarding alcohol consumption and tamper information with the ability to download data via standard telephone line, Ethernet, or wirelessly, and also have ability for agency staff to directly download bracelet data to agency computers such as via a direct USB data transfer, or other methodology, on clients where land line and cellular coverage is not available or is not the preferred communication method by agency personnel. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE



The SCRAM CAM bracelet can store up to 160 days of events in its onboard memory. In addition, the base station has its own memory capacity and can store up to a month's worth of data (about 7,500 messages). All messages are time-stamped and stored in the non-volatile memory, so that the messages are never lost. Sentinel offers landline, *cellular/Wi-Fi*, and *ethernet-based base stations / receivers* for use with the SCRAM CAM bracelet. Data can also be retrieved using the SCRAM CAM Direct Connect device. This enables the supervising authority to connect the SCRAM CAM bracelet directly to an Internet-enabled computer without the need for the SCRAM Base Station and phone line.

The bracelet communicates all alerts with the base station when in range, which then sends all available data to the monitoring system. At a pre-scheduled time(s) each day, the SCRAM CAM bracelet "communicates" with the base station, which then retrieves all available data from the bracelet and sends it for review. The base station also downloads monitoring and reporting schedules to the bracelet. Additionally, the SCRAM CAM base station is available with **Ethernet connectivity** to allow the unit to communicate over the internet using the participant's home modem. The Ethernet port at the back of the base station connects to almost all modems, regardless of internet service provider. Ethernet connectivity is a modern alternative to landline communication.

In cases where a program participant may be required to report to agency personnel on a weekly basis, he or she can come into the supervising authority's office to have data that has been stored in the bracelet downloaded via the SCRAM CAM Direct Connect device. The compact Direct Connect device is slipped over the participant's bracelet (while worn) and attached by USB cable to an internet-enabled computer. The stored information is then transmitted from the SCRAM CAM bracelet directly for review without the need for a base station.

- Contractor must provide a centralized and controlled data center and support staff that monitors client information received via the internet and provides analysis of and notifications to agency staff of alcohol readings, tamper alerts, communication failures, equipment issues, maintenance needs and/or malfunctions. The monitoring center must be available on a 24/7 basis, 7 days per week, 365 days per year.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained technicians and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

Our monitoring centers are staffed 24 hours a day, 7 days a week with live staff including a supervisor always on duty and certified operators cross-trained to support our suite of supervision services and monitoring products. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year. **There is no subcontracting of any of our proposed monitoring services.**



Sentinel provides access to designated **Help Desk** staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. Sentinel provides toll-free telephone access, toll-free fax line, and email access to over 60 operators and customer service representatives, available to officers 24 hours a day, 7 days a week, 365 days a year, who can resolve most technical problems over the telephone or through remote diagnostics.

Sentinel strives to resolve all customer inquiries promptly and on first contact. Each monitoring center operator has the expertise to easily identify, explain, and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert and changing a participant's schedule.

In addition, this specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

- The system must include inventory tracking and management features.

SENTINEL RESPONSE

SCRAM Optix is accessible 24/7 via any web-enabled device allowing officers to enroll clients, adjust device settings, enter/edit schedules, select notification methods or parameters, manage inventory, and quickly assess detailed caseload information at-a-glance via device and status indicators.

- The Contractor must archive and retain archived data for a period of five (5) years from the date the client is enrolled in the system.

SENTINEL RESPONSE

SCRAM Systems will archive and retain archived data for a period of five (5) years from the date the client is enrolled in the system.

- Contactor's system must provide date and time stamped readings once every 30 minutes or less of Transdermal Alcohol Concentration, body temperature and attempts to obstruct readings of the device.

SENTINEL RESPONSE

SCRAM CAM is the only CAM device on the market that uses a controlled, quantifiable sampling method—collecting every second—to create a measured sample every 30 minutes including data and time stamped readings. This is the same proven type of sample delivery system used in evidential breath testing equipment that has been the standard in law enforcement for decades. Without this sampling method, a device is susceptible to environmental factors causing false positives and/or may require a secondary test. By combining this system with SCRAM Systems' patented method of "contaminant isolation" SCRAM CAM can distinguish between environmental and ingested alcohol.



The sample delivery method results in a quantifiable Transdermal Alcohol Concentration (TAC) curve, with specific alcohol absorption and elimination rates. The contaminant isolation method allows SCRAM CAM to measure the level of environmental or ambient alcohol prior to each transdermal alcohol measurement, indicating if a test has been contaminated. In addition, before every 30-minute measurement, SCRAM CAM tests the ambient air around the device to determine if environmental alcohol is present.

Additionally, the bracelet is capable of identifying proximity tampering—situations where foreign objects or barriers are placed between the bracelet and the skin to obstruct its function. These sensors continuously monitor for changes in temperature, interruptions in skin contact, and any attempts to cut, block, or remove the bracelet.

- A daily summary or action plan must be provided daily, which reports the status of any clients in violation of the program or in need of technical maintenance.

SENTINEL RESPONSE

The Daily Activity Plan (DAP), which can be automatically delivered up to twice daily, shows which participants had specific violations or are in need of technical maintenance. All alerts and monitoring activities are also accessible through the software and are automatically date- and time-stamped.

Prior to notification, SCRAM-certified analysts confirm all CAM-specific violations (drinking events, tampers, obstructions, communication alerts, and environmental contaminants/alcohol). This ensures that alerts are valid, so that follow-up testing —such as blood, breath, or urine—are not needed to confirm drinking events.

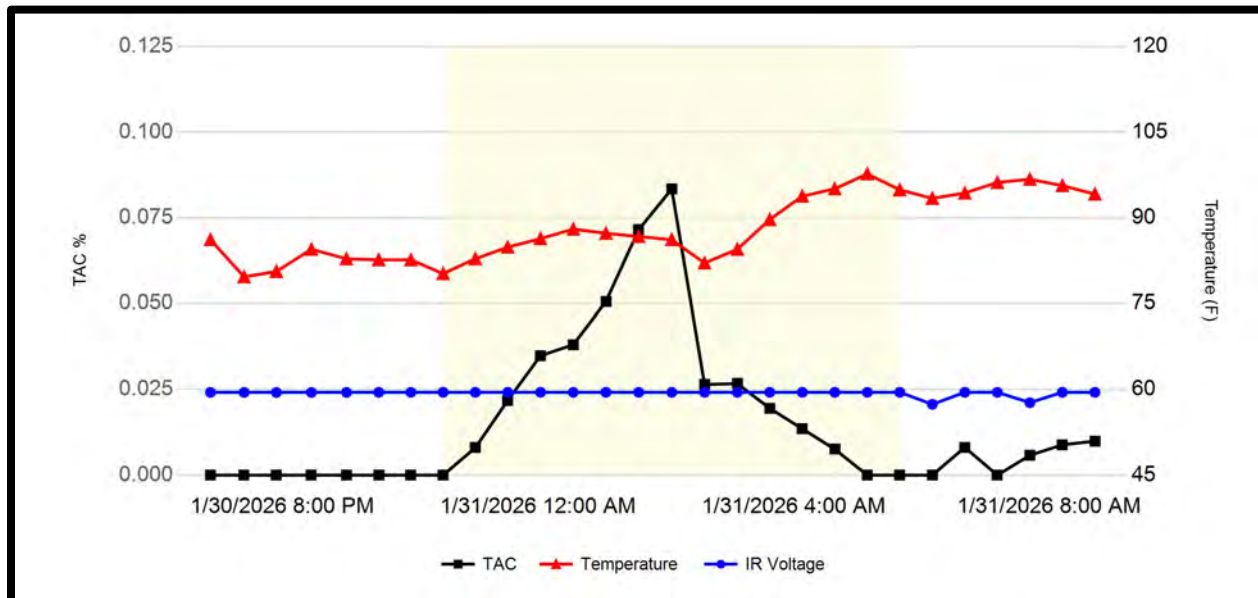
- The system must provide easy-to-read non-compliance reports that include detailed information outlining any presence of alcohol displayed graphically and numerically to indicate ~~approximate the~~ time of ingestion and the Transdermal Alcohol Concentration (TAC) present in the system over the time of the event. **[Edited per Amendment # 3, Scope of Work_Revised 2.6.26~2]**

SENTINEL RESPONSE

The Daily Activity Plan provides easy-to-read non-compliance reports with clear graphs that illustrate a drinking event with date and time of the alcohol consumption from absorption through elimination. As shown in the following graph, Transdermal Alcohol Concentration (TAC) is represented by the black line. Tamper detections, in the form of an infrared (IR) sensor (represented by the blue line) and temperature reading (represented by the red line) appear on the graph along with the TAC readings.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- Summary management reports regarding individual clients, dates of system use, agency-wide equipment inventory status, and billing details provided upon request in an easy-to-read format.

SENTINEL RESPONSE

Sentinel will provide each Participating Entity with summary management reports regarding individual clients, dates of system use, agency-wide equipment inventory status, and billing details provided upon request in an easy-to-read format.

3. CAM Customer Support and Training

3. Customer Support and Training

- The Contractor must provide a dedicated account representative.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

As a leading provider of electronic monitoring services and as a NASPO ValuePoint contractor for more than 25 years, Sentinel has established processes and protocols to effectively deliver services via NASPO ValuePoint agreements. Sentinel will continue to ensure familiarity with the Master Agreement including all terms and pricing.

The NASPO ValuePoint Agreement will receive full attention of Sentinel's Senior Leadership team as evidenced by the fact Sentinel is appointing Mr. Mike Dean, Sentinel's Senior Vice President of Sales as the point of contact for the NASPO ValuePoint Master Agreement.

MIKE DEAN | Senior Vice President of Sales

- + Mr. Dean oversees all Sentinel sales personnel and manages the company's cooperative purchasing agreements. With over 33 years in the electronic monitoring industry overseeing sales and contracting for some of the largest electronic monitoring providers, including BI Incorporated, 11 years, G4S Justice



Services, 7 years, and Sentinel for the past 14 years, Mr. Dean has unparalleled expertise in collaborating with Federal, State, and Local Governments, developing electronic monitoring programs and leveraging cooperative purchasing to the benefit and convenience of government agencies.

- + Mr. Dean has worked directly with procurement departments negotiating Participating Addendums and reviewing contractual requirements for entities that makes him an exceptional subject matter expert and primary point of contact for the NASPO ValuePoint Cooperative Purchasing Agreement. Mr. Dean holds a Bachelor Agreement in Criminal Justice, from the University of Cincinnati, and as Senior Vice President of Sales, Mr. Dean is strategically positioned to champion the NASPO ValuePoint agreement. He will provide oversight for the NASPO ValuePoint Master Agreement and for the agency's participating addendums, programs and purchasing department, while also facilitating all post-award implementation adjustments required for this contract.

Mr. Dean will work closely with the Sentinel Field Operations Team and have complete support from our Chief Operating Officer, Mr. Darryl Martin. Mr. Martin has been overseeing the delivery of electronic monitoring services to the NASPO ValuePoint Agreements for more than 25 years. Mr. Martin will exercise all Sentinel departments and employee base of more than 280 to ensure complete compliance with the Master Agreement including the following resources that stand ready to continue providing services.

Mrs. Melissa Staff, Sentinel's Senior Vice President of Field Operations, is responsible for the management and oversight of our Regional Account Management team as well as Sentinel's national network of customer support and branch office personnel. Her team manages the day-to-day needs of our benchmark offender-funded programs as well as providing customer service to our agency-funded contracts across the United States. **A dedicated account representative will be assigned to each Participating Agency for the duration of contract operations.** The Sentinel account representative will be responsible for:

- + Account retention;
- + Being the main liaison between the Customer and Sentinel;
- + Providing consultative account management practices to government channel accounts in their region to ensure best practices are in place;
- + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
- + Introduction and socialization of hardware and software offerings that may benefit the Customer;
- + Conducting training and overseeing the implementation; and
- + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.

- The Contractor must provide support functions 24/7/365.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained technicians and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

Our monitoring centers are staffed 24 hours a day, 7 days a week with live staff including a supervisor always on duty and certified operators cross-trained to support our suite of supervision services and monitoring products. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since



operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year. **There is no subcontracting of any of our proposed monitoring services.**

Sentinel provides access to designated **Help Desk** staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. Sentinel provides toll-free telephone access, toll-free fax line, and email access to over 60 operators and customer service representatives, available to officers 24 hours a day, 7 days a week, 365 days a year, who can resolve most technical problems over the telephone or through remote diagnostics.

Sentinel strives to resolve all customer inquiries promptly and on first contact. Each monitoring center operator has the expertise to easily identify, explain, and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert and changing a participant's schedule.

In addition, this specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

- The Contractor must provide toll free access to customer support/monitoring center.

SENTINEL RESPONSE

As stated above, Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained operators and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

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

In the unlikely event that problem solving requires a higher-level of involvement, Sentinel's customer service is equipped with all necessary computer equipment and staffed by experienced technicians, as well as the engineers who developed the system technology, who can quickly analyze and resolve the problem.

- The Contractor must provide initial start-up training that must include but not be limited to the following:
 - o The enrollment of clients into the software system.



- o The installation, use, de-installation, and cleaning of the equipment.
- o The generation and interpretation of data/monitoring reports.
- o Accessing/using Contractor's technical support/help menus and monitoring center.

SENTINEL RESPONSE

Sentinel understands that training and customer service are crucial to the success of any electronic monitoring program, and Sentinel is dedicated to meeting those needs. Sentinel agrees to provide the initial training session and ongoing training, including all manuals, concerning the implementation and management of the monitoring program as determined by the contract. Sentinel is committed to establishing a partnership over the term of the contract to ensure that all staff members are fully and properly trained. Training is offered for the life of the program as outlined in the monitoring services agreement at no additional cost.

Sentinel's training philosophy for our instructor-led courses can be a combination of respondent training as well as train-the-trainer if so desired by the Participating Entity. We work to provide all training for our customers based on their individual programmatic needs and thus will work with the Participating Entity to develop and deliver a training format that provides the best solution for each training location. Sentinel's standard training minimally includes the following items: installation and de-installation of equipment; maintenance and cleaning of equipment; use of web-based information system including procedures for enrollment and curfew changes as well as the generation and interpretation of reports; troubleshooting monitoring problems; accessing our technical support and monitoring center; and any additional training as needed to remain current on monitoring equipment and web-based information system.

Sentinel's implementation team will train all agency personnel assigned to the program prior to deployment and as needed for changes to the system, equipment, web-based information system, or personnel, for the duration of the program as directed by the contract. Our standard training protocol includes demonstration, discussion, and hands-on sessions on the following topics:

- + All RF, GPS, Alcohol Monitoring equipment, and client app solutions (use, installation, removal, and troubleshooting)
 - + Enrollment (enrollment, deactivation, and the setting of all monitoring parameters including curfew schedules and GPS zones)
 - + Tracking and monitoring of participants
 - + Alarm processes and resolution procedures (agency-specific protocols)
 - + Notification processes and reports (agency-specific protocols)
 - + Monitoring System (complete instruction on the use of the web-based information system including, but not limited to, participant enrollment, modifications, reports, schedules, advanced automated analytics, location review, and deactivations)
 - + Interpretation of Monitoring Reports (review, define and interpret daily monitoring activity, and Glossary of Terms/definitions)
 - + Mobile Application (complete instruction on the use of the Mobile App including, but not limited to, participant information modifications, schedules, location review, device command initiation, field contacts, equipment inventory, and reports/activity review)
 - + Accessing Technical Support and Help Desk Services (contact information and access to training support materials)
-
- The Contractor must provide materials and brochures on the use of the equipment and system.

SENTINEL RESPONSE



Sentinel will provide all user guides, user manuals, brochures, PowerPoint presentations, reference guides, and training videos on the use of the equipment and system for each Participating Entity. Additionally, Sentinel will provide instruction and hand-out material for agency staff to instruct program participants on the use, care, and charging of the equipment.

- The Contractor must provide on-going and supplemental training offerings either on-site or via web-based programs at a minimum of once (1) per year after the initial start-up training offerings or on an as needed basis, based on any significant changes to the Contractor provided equipment and/or technology.

SENTINEL RESPONSE

In addition to the initial training and set up process with a representative on location, the Sentinel Training Department offers either on-site or via webinar training sessions for customers and staff at a minimum of once (1) per year after the initial start-up training offerings, on an as-needed basis, or based on any significant changes to equipment and/or technology. This training is offered for all technologies and services including those proposed herein. It is important to note that Sentinel's webinar training sessions involve interactive voice plus visual contact with a live Sentinel expert trainer, therefore trainees can ask questions and engage in discussion with the trainer as part of any webinar.

Training and webinars are offered at no additional cost to the Participating Entity based on internal training calendars, individual training needs, and scheduled on demand. Webinars are conducted based on contract specifications and/or training needs and can include training on equipment, services, software, web-based system changes, and/or updates. Training is offered for the life of the program as outlined in the Master Agreement. At any time, a Participating Entity can contact our Help Desk for additional support to ensure they are maximizing the technology solution to its fullest potential.

B. REMOTE ALCOHOL MONITORING (RAM)

1. BAT Hardware

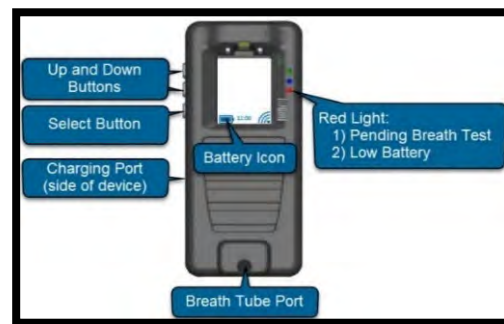
B. Remote Alcohol Monitoring (RAM)

1. Hardware

SENTINEL RESPONSE

REMOTE BREATH PRO

For the Remote Alcohol Monitoring product needs, Sentinel is proposing the use of two products providing Participating Entities choice when working with Sentinel. For Remote Alcohol monitoring Sentinel is proposing the SCRAM Remote Breath Pro, a portable wireless breath alcohol monitoring device that provides a GPS location with both taken and missed tests. The device communicates via cellular networks and notifies supervising authorities of any alcohol readings (BrAC), tamper alerts, or possible equipment malfunctions so they can quickly respond. The Remote Breath Pro offers the following features and benefits:



- + Sleek, lightweight, and compact. The device measures 2.9"x6.5" with a 1.2" depth.



- + Facial authentication decreases officer photo manual matching by up to 95%, allowing officers more time to spend on their caseloads and participants.
- + Enhanced facial guidance provides visual cues ensuring face is aligned during participant testing
- + Device-initiated testing—automatically turns on and prompts participants for scheduled and on-demand tests.
- + Wi-Fi capability so that downloads can be performed when a cellular connection is not available.
- + Store and Forward—never lose test results.
- + GPS location with both taken and missed tests.

SHADOWBRIETY (OPTIONAL)

Sentinel has also proposed **as an option** Shadowtrack ShadowBriety, a comprehensive supervision tool designed for participants required to submit to alcohol testing as a stand-alone system or in conjunction with Shadowtrack Phone App and Interactive monitoring as a graduated sanction.

With ShadowBriety, participants are checked regularly, randomly, or in the moment, for breath alcohol levels. Through facial recognition and Bluetooth technology, results are immediate, accurate, and specific to the participant. Highlights of the unit include:

- + Provides sobriety testing through the inclusion of the ShadowBriety - BACtrack Portable Breath Alcohol Testing Device
- + Through facial recognition and Bluetooth technology, results are immediate, accurate, and specific to the participant
- + Captures the participant's BAC level along with a GPS location of each Sobriety test
- + Utilizes facial recognition for participant identity confirmation
- + Test schedule options include random, fixed time, and on demand
- + Results Documented within the Monitoring Application
- + Frequency Determined by Officer
- + caseload/dashboard
- + Caseload Management Integration
- + Anti-Spoofing Technology Built In



- Device must be capable of performing a deep-lung breath specimen, fixed, random, and on-demand tests, or be programmable to perform a combination of these test types. Device must be a Handheld Device Capable of Testing in all locations.

SENTINEL RESPONSE

REMOTE BREATH PRO

The Remote Breath Pro alcohol testing unit is a hand-held device that will perform a deep-lung breath specimen using an electrochemical fuel cell that has been validated through decades of research and experience. It is considered the most reliable in alcohol testing applications. This is the same fuel cell used in evidential breath testing and interlock devices and consists of extremely sensitive ethanol-specific alcohol sensors. Remote Breath



Pro offers unlimited flexible testing schedules including random, scheduled, and on-demand options. Authorized agency staff will have the option of remotely programming the device to perform any combination of these types of tests.

The device also offers flexible notification to clients to alert them when it is time to take a test. These alerts can be sent audibly or via vibrations through the device. Breath test reminders can be sent automatically to the client's cell phone via text message at customizable time frames, such as 15 minutes prior to a test time. For positive tests, SCRAM Remote Breath Pro will prompt the client to complete a secondary confirmation test, which the agency can set to take place between 10 and 30 minutes after the initial positive test.

Remote Breath Pro uses the AT&T LTE network with a cellular modem that is supported by both 4G and 5G networks. Additionally, Remote Breath Pro has been enhanced to have Wi-Fi capabilities, so that clients without cell coverage can use home or public Wi-Fi to transmit test results.

SHADOWBRIETY (OPTIONAL)

With ShadowBriety, participants are tested via fixed, random, and/or on demand, tests for breath alcohol levels via the use of the BACtrack handheld remote alcohol monitoring device. When alcohol is consumed, it is absorbed from the mouth, throat, stomach, and intestines into the bloodstream. Blood carries alcohol throughout the body - including the lungs. As alcohol-laden blood moves across the membranes of the lung's air sacs (alveoli), it permeates the breath. The concentration of alcohol in the alveolar air is directly related to the concentration of alcohol in the blood and through a deep-lung breath specimen, the device can accurately detect and report alcohol consumption. Through facial recognition and Bluetooth technology, the alcohol results are immediately and accurately confirmed to be specific to the program participant through facial recognition and reported and stored on the monitoring application.

The device also offers flexible notification to clients to alert them when it is time to take a test. These alerts can be sent audibly or via vibrations through the participant's mobile phone. Breath test reminders can be sent automatically to the client's cell phone via text message at customizable time frames, such as 15 minutes prior to a test time. For positive tests, ShadowBriety automatically prompts the client to complete a secondary confirmation test, which the agency can set to take place between 10 and 30 minutes after the initial positive test.

ShadowBriety uses Bluetooth technology to pair with the participants mobile phone that is supported by available cellular networks including 4G LTE and 5G networks.

- Device must be capable of storing test results in the RAM's memory.

SENTINEL RESPONSE

REMOTE BREATH PRO

Remote Breath Pro incorporates a "Store & Forward" feature, which ensures a test is never missed. Its memory can store up to 48,000 test results when participants are out of cell service. The time-stamped results are forwarded as soon as coverage is regained.

SHADOWBRIETY (OPTIONAL)

ShadowBriety uses Bluetooth technology to pair the BACtrack device to the participant's mobile smartphone (compatible with both Apple iOS and Android devices) to create a reliable communication connection by leveraging the smartphone communication capabilities and its RAM memory capacity. ShadowBriety uses a professional-grade fuel cell sensor to analyze the participants' breath, then transmits this reading to the mobile smartphone, where the Blood Alcohol Content (BAC) estimate is communicated to the monitoring application. The

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



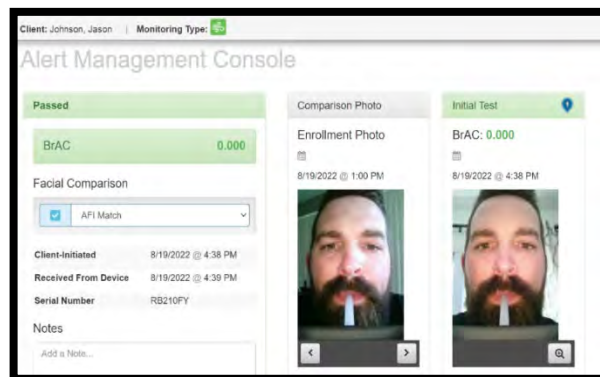
BACtrack device is powered by a battery that can be recharged via the micro-USB cable provided, similar to the smartphone.

- Device must use facial confirmation software, or similar verification method, to confirm participant's identity. **[Edited per Amendment # 3, Scope of Work_ Revised 2.6.26~2]**

SENTINEL RESPONSE

REMOTE BREATH PRO

The Remote Breath Pro device captures participant images with a 5-megapixel, high-resolution camera and the Automated Facial Intelligence (AFI) system uses facial matching to automatically examine and compare the images. AFI is the same facial authentication technology used internationally by government security forces. The system automatically scans and confirms the participant's identity with each breath test to eliminate manual matching of photos by up to 95%. Facial matching technology eliminates the need to scroll through numerous photos, increasing accuracy and efficiency, and reducing risk. It enables real-time notifications when the participant does not match and allows the officer to immediately address a potential violation.



SHADOWBRIETY (OPTIONAL)

Shadowtrack's biometric technology used with the ShadowBriety records high-resolution video and audio – offering unbeatable clarity and transparency. A participant's identity is reliably identified via enhanced facial recognition technology that allows authorized agency staff to review all test recordings and audio records.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Shadowtrack's biometric technology incorporates FACEdetect™ that Verifies that each test is being taken on camera. Should supervising personnel learn of any changes to the participant's appearance, Shadowtrack allows for an update to the existing facial print.



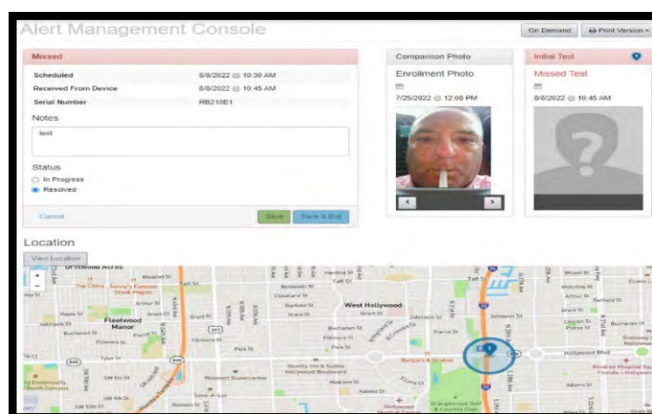
ShadowBriety Other devices

- Device must ~~combine-continuous~~ collect the GPS location during the tracking with remote breath alcohol testing. [Edited per Amendment # 3, Scope of Work_ Revised 2.6.26~2]

SENTINEL RESPONSE

REMOTE BREATH PRO

The Remote Breath Pro device automatically powers itself up during test windows and tracks its location at the time of the scheduled test. The device provides a GPS location with every test—both taken and missed tests. A GPS location with a missed test is especially useful as it can help an officer make a more informed decision as to why a participant missed a test. For example, participants often state they missed a test because they left their device at another location. Officers can verify or refute the participant's claim by comparing the GPS point on a missed test (verified via GPS ping) with the participant's location.



SHADOWBRIETY (OPTIONAL)

The ShadowBriety collects the location each time a test is taken and uploads the BAC test results and the location of the test. Below, the software application screenshot shows the location of a participant's BAC test.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Through the use of Google Maps, the agency can zoom in to observe the location where the breath test was taken.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Sobriety Results

	Image	Date	Sobriety Result	Facial Result
1		9/22/2025, 7:53 PM	Score 0.0000 Result Success	Score 100.00 Result Success

1 to 1 of 1

Call Location

Map

Satellite

Terrain



Call Location

Map

Satellite



- Device must use Wi-Fi technology as an alternative when cellular communication is unavailable at the wearer's residence and as a reliable location source when GPS is unavailable or impaired.

SENTINEL RESPONSE

REMOTE BREATH PRO

Remote Breath Pro uses the AT&T LTE network with a cellular modem that is supported by both 4G and 5G networks. Remote Breath Pro has been enhanced to have Wi-Fi capabilities, so that participants without cell coverage can use home or public Wi-Fi to transmit test results.

—IMPORTANT ADVANTAGE—

Because Remote Breath Pro stores the participant's test schedule on the device, it automatically turns on and prompts participants for scheduled and on-demand tests—even when out of cell coverage. Notification for both BrAC and positive participant ID is immediate. Additionally, Remote Breath Pro incorporates a "Store & Forward" feature, which ensures a test is never missed. Its memory can store up to 48,000 test results when participants are out of cell service. The time-stamped results are forwarded as soon as coverage is regained.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SHADOWBRIETY (OPTIONAL)

ShadowBriety uses Bluetooth technology to pair the BACtrack device to the participants mobile smartphone and (compatible with both Apple iOS and Android devices) to create a reliable communication connection by leveraging the smartphone communication capabilities and its RAM memory capacity. ShadowBriety can use Wi-Fi as an alternative when 4G LTE and/or 5G networks are not available. The BACtrack device is powered by a battery that can be recharged via the micro-USB cable provided, similar to the smartphone.

- Device must be lightweight, discreet, and easy to use, providing test notifications through push technology or SMS.

SENTINEL RESPONSE

REMOTE BREATH PRO

The handheld device is sleek, lightweight, and compact, measuring 2.9" x 6.5" with a 1.2" depth and weighing only 9.95 ounces. The small and durable device comes with a fitted protective carrying case and adapts to the participant's everyday life, enabling participants to take a test anytime, anywhere. Testing schedules and notifications are pushed to the device, and officers have the option to schedule reminders to be sent via text message to the client's cell phone shortly before or at the test time. Text messages can also be sent for "Battery Low" and "Battery Critically Low" alerts to help the client avoid a power fail situation and prevent unnecessary alerts to the officer. The automated courtesy reminders can be sent in English or Spanish.



—IMPORTANT ADVANTAGE—

Remote Breath Pro stores the participant's test schedule on the device and automatically turns on and prompts participants for scheduled and on-demand tests—even when out of cell coverage. Additionally, Remote Breath Pro incorporates a "Store & Forward" feature, which ensures a test is never missed.

The device is easy and simple to use, with clear instructions on the display screen and side-buttons to scroll up or down and select menu options. Participants can also adjust the volume and screen brightness as preferred.

SHADOWBRIETY (OPTIONAL)

ShadowBriety includes the BACtrack remote alcohol monitoring device that lightweight, discreet, and easy to use, measuring 1.75 x 2.75 x 0.63 inches and weighing 1.75 oz. and provides test notifications through push technology or SMS.



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474

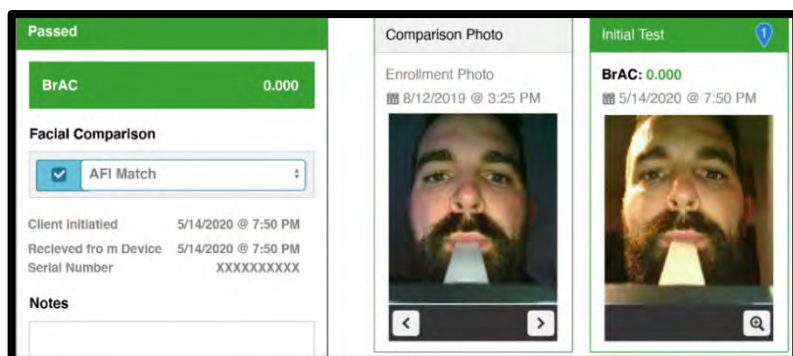


- Device must provide a numeric result that represents the participant's breath alcohol concentration (BrAC) and accurately corresponds to the participant's blood alcohol concentration (BAC).

SENTINEL RESPONSE

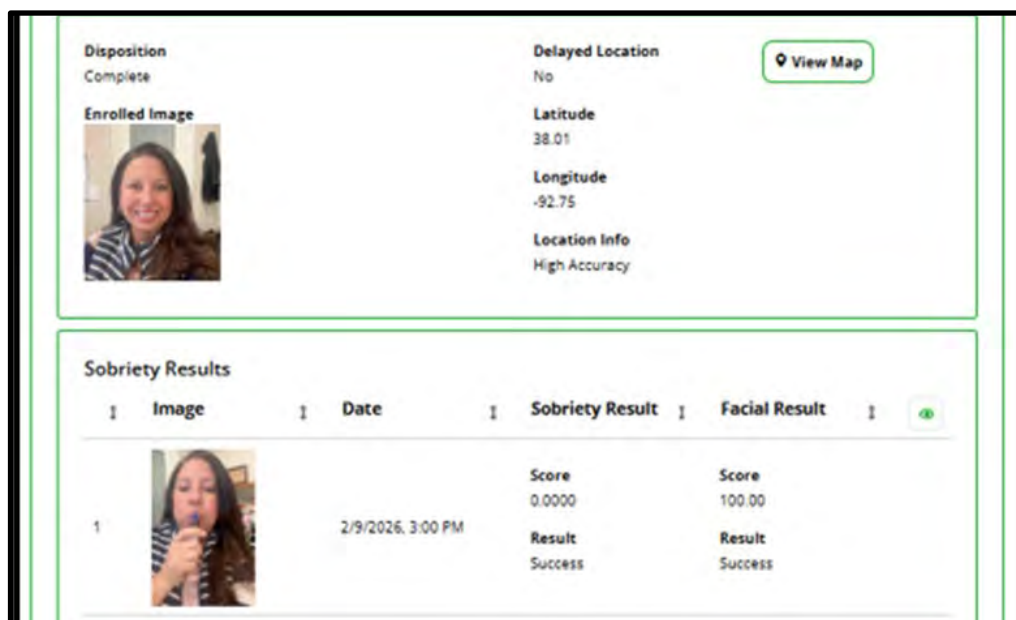
REMOTE BREATH PRO

As shown in the screen image below, Remote Breath Pro provides a numeric result that represents the participant's breath alcohol concentration (BrAC) and accurately corresponds to the participant's blood alcohol concentration (BAC).



SHADOWBRIETY (OPTIONAL)

The Shadowtrack ShadowBriety shows BAC readings for all alcohol monitoring test results. It utilizes a professional-grade fuel cell sensor and is designed to reliably monitor the abstinence of alcohol. As shown in the screen image below, ShadowBriety provides a numeric result that represents the participant's breath alcohol concentration (BrAC) and accurately corresponds to the participant's blood alcohol concentration (BAC) as seen in the below image.



**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



By selecting a Sobriety test from the Compliance tab, authorized users can review the details of the test including the participant's BAC as well as the test image/enrollment image and the GPS location where the test occurred. If the test was non-compliant, the reason for the non-compliance will be displayed in the test details. Additionally, users can also add notes to the test record.

- Device must transmit equipment status data, including, but not limited to, calibration status, equipment and battery condition, power and telephone line connects and disconnects, and tamper status. All data reported shall be time-stamped.

SENTINEL RESPONSE

REMOTE BREATH PRO

With each transmission to the supporting monitoring system, Remote Breath Pro transmits the device calibration status, equipment and battery condition, power and cellular communication connects and disconnects, and tamper status. Additionally, when applicable, the unit reports the real-time BrAC level, GPS data, and verification of client's identity at the time of the test. All data reported is date and time stamped for historical accuracy.

SHADOWBRIETY (OPTIONAL)

The Shadowtrack ShadowBriety monitoring application includes a Device Tab, where supervising personnel can perform various service/command functions in order to efficiently monitor device functionality as well as to communicate with the device and/or participant. For example, supervising personnel can see vital information such as the last device communication, device battery status, etc. Additionally, the following commands can be performed when under this tab as well: Send Message, Call, Suspend, Unassign Device, Request Location.

- Device must have a rechargeable battery.

SENTINEL RESPONSE

REMOTE BREATH PRO

The Remote Breath Pro is powered by a rechargeable Lithium-Ion battery. The device typically lasts two (2) days in between charges. The participant is alerted by light indicators, text message, and/or audible alarm when the battery is low.

The device is easily charged using modern and simple charging methods. It has a USB-C charging port and comes with a USB cable and adapter. Participants can connect the device to the included adapter and plug it into any standard wall outlet or simply charge it with a USB port using the supplied USB cable. A log is created in the information system showing a date and time stamped list of every time the device is charged. Officers can see the participant's specific charging patterns and tell how long a device was plugged in to determine if the participant is charging the device on a regular basis.

SCRAM [®] SYSTEMS Remote Breath Battery Charge Summary 8/29/2022 thru 9/15/2022					
Client:	Smith, Jillian		Caselead:	Adams County	
Case Number:	CA-2022-13-7-RB		Agent:	Miller, Phil	
Date of Birth:	1/17/1970		Court:	Douglas County Court	
			Judge:	Anderson, Judge	
Event	Plug In Time	Un Plug Time	Charge Time (dd:hh:mm:ss)	Reached Full Charge	
Plug In	8/31/2022 8:51 AM	8/31/2022 1:00 PM	0:04:09:14	Yes	
Plug In	9/2/2022 8:44 PM	9/6/2022 8:02 AM	3:11:18:16	Yes	
Plug In	9/8/2022 7:45 AM	9/8/2022 7:56 AM	0:00:10:47	Yes	
Plug In	9/8/2022 7:59 AM	9/8/2022 10:49 AM	0:02:49:47	Yes	
Plug In	9/8/2022 2:32 PM	9/9/2022 8:28 AM	0:17:55:20	Yes	
Plug In	9/12/2022 11:15 AM	9/13/2022 7:54 AM	0:20:38:37	Yes	
Plug In	9/15/2022 5:36 AM	9/15/2022 10:54 AM	0:05:18:18	Yes	



SHADOWBRIETY (OPTIONAL)

The ShadowBriety is powered by a rechargeable Lithium-Ion battery and is rechargeable with the included micro-USB cable. The devices will operate for five (5) days between charges.

2. BAT Software

2. Software

- Immediate Reporting/Notification via cellular of Deep Lung Sample Breath Alcohol Content plus Color Participant Image and GPS Mapping of Participant Location at Time of Each Test

SENTINEL RESPONSE

Results are immediately reported after each test according to agency-defined procedures. Both Remote Breath Pro and/or the ShadowBriety device provide real-time BrAC level, GPS data, and verification of client's identity with color image at the time of the test. The facial authentication software alerts the officer if someone besides the client is taking the test.

- Scheduled, Random & On-Demand Testing

SENTINEL RESPONSE

Remote Breath Pro and the ShadowBriety devices offer unlimited flexible testing schedules including random, scheduled, and on-demand options. The devices also offer flexible notification to clients to alert them when it is time to take a test. These alerts can be sent audibly or via vibrations through the Remote Breath Pro device. Both devices allow for breath test reminders to be sent automatically to the client's cell phone via text message at customizable time frames, such as 15 minutes prior to a test time.

For positive tests, Remote Breath Pro will prompt the client to complete a secondary confirmation test, which the agency can set to take place between 10 and 30 minutes after the initial positive test. When using ShadowBriety, the user agency can establish customizable retest times to complete secondary confirmation tests in the event of a positive test result.

- Tamper-Detect Features

SENTINEL RESPONSE

REMOTE BREATH PRO

Remote Breath Pro ensures accuracy by using security-grade facial authentication software to detect attempts to circumvent the system. The system automatically scans and confirms each participant's identity with each breath test. In addition, if the battery case is opened, a Device Housing Breach alert will be generated. Attempts to tamper with or circumvent the system will be reported per predefined agency procedures.

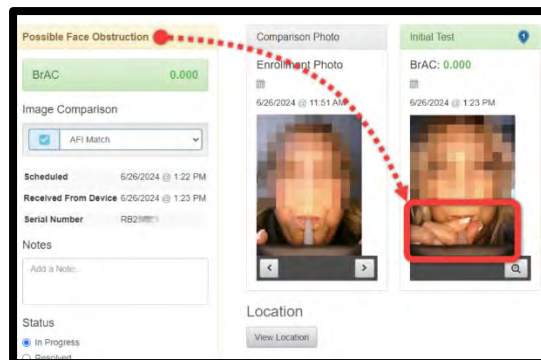
**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The device also has **automatic obstruction scanning** and will trigger a Possible Face Obstruction alert if irregularities are detected with the breath tube during the breath test photo. These include, but are not limited to:

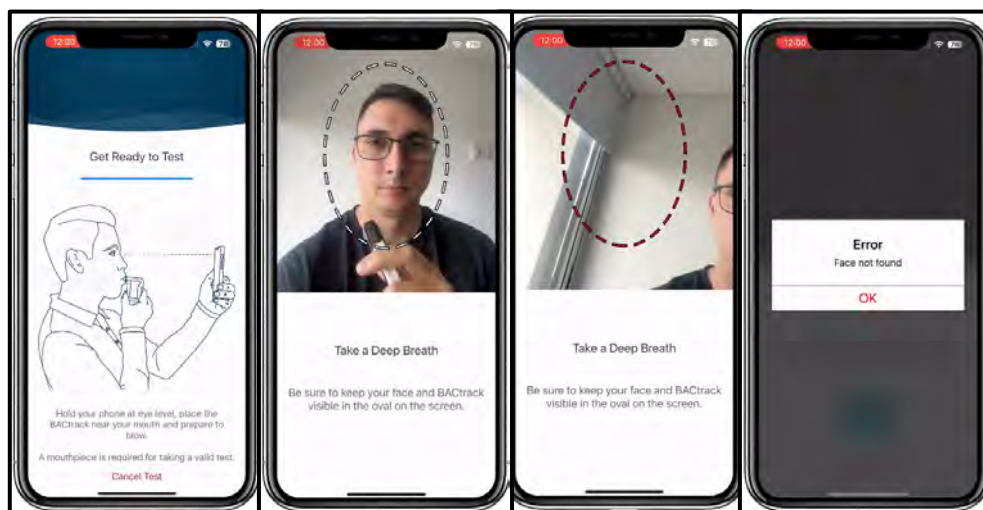
- + Any part of the straw being obstructed from the camera's view, such as by hands, fingers, clothing, or the Remote Breath Pro case itself.
- + Not using the provided straw, leading to irregularities in the color, size, or shape of the breath tube.
- + Modifications to the straw, including any attachments connected to it.
- + The straw not being in the client's mouth or being entirely missing.



SHADOWBRIETY (OPTIONAL)

Shadowtrack's biometric technology incorporates security features that verify that each test is being taken on camera.

- + Uses advanced facial detection technology to verify that a visible face is present, if No face detected, or if Tester is not facing forward, and the test is being blocked
- + Designed to prevent tampering, the test also stops if it detects more than one face.
- + Designed to keep every test honest by requiring the tester to show their face and preventing multiple faces on-screen.
- + Advanced features that confirm the participant is blowing into the breath tube securely attached to the ShadowBriety - BACtrack device.





- Automated notifications and alerts (via SMS, email, or in-platform) for violations such as tampering, missed tests, positive test, or low battery.

SENTINEL RESPONSE

REMOTE BREATH PRO

For the Remote Breath Pro device, the officer for the Participating Entity will receive automated notifications and alerts via SMS, email, and/or in the platform as defined by the agency, for violations such as tampering, missed tests, positive tests, or low battery. Authorized agency staff will have the ability to determine which violations/events must trigger notifications and by what means the notifications must be sent to agency personnel as well as enter information to initiate multiple alert notifications, e.g., agency officers, law enforcement) for specified key events or non-compliance of the monitoring parameters.

SHADOWBRIETY (OPTIONAL)

For the Shadowtrack ShadowBriety device, the officer for the Participating Entity will receive automated notifications and alerts via SMS, email, and/or in the platform as defined by the agency, for violations such as tampering, missed tests, positive tests, or low battery. Authorized agency staff will have the ability to determine which violations/events must trigger notifications and by what means the notifications must be sent to agency personnel as well as enter information to initiate multiple alert notifications, e.g., agency officers, law enforcement) for specified key events or non-compliance of the monitoring parameters.

3. BAT Customer Support and Training

3. Customer Support and Training

- The Contractor must provide a dedicated account representative.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

As a leading provider of electronic monitoring services and as a NASPO ValuePoint contractor for more than 25 years, Sentinel has established processes and protocols to effectively deliver services via NASPO ValuePoint agreements. Sentinel will continue to ensure familiarity with the Master Agreement including all terms and pricing.

The NASPO ValuePoint Agreement will receive full attention of Sentinel's Senior Leadership team as evidenced by the fact Sentinel is appointing Mr. Mike Dean, Sentinel's Senior Vice President of Sales as the point of contact for the NASPO ValuePoint Master Agreement.

- + Mr. Dean oversees all Sentinel sales personnel and manages the company's cooperative purchasing agreements. With over 33 years in the electronic monitoring industry overseeing sales and contracting for some of the largest electronic monitoring providers, including BI Incorporated, 11 years, G4S Justice Services, 7 years, and Sentinel for the past 14 years, Mr. Dean has unparalleled expertise in collaborating with Federal, State, and Local Governments, developing electronic monitoring programs and leveraging cooperative purchasing to the benefit and convenience of government agencies.
- + Mr. Dean has worked directly with procurement departments negotiating Participating Addendums and reviewing contractual requirements for entities that makes him an exceptional subject matter expert and primary point of contact for the NASPO ValuePoint Cooperative Purchasing Agreement. Mr. Dean holds a Bachelor Agreement in Criminal Justice, from the University of Cincinnati, and as Senior Vice President of Sales, Mr. Dean is strategically positioned to champion the NASPO ValuePoint agreement. He will provide corporate oversight for the agency's participating addendums, programs and purchasing department, while also facilitating all post-award implementation adjustments required for this contract.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Mr. Dean will work closely with the Sentinel Field Operations Team and have complete support from our Chief Operating Officer, Mr. Darryl Martin. Mr. Martin has been overseeing the delivery of electronic monitoring services to the NASPO ValuePoint Agreements for more than 25 years. Mr. Martin will exercise all Sentinel departments and employee base of more than 280 to ensure complete compliance with the Master Agreement including the following resources that stand ready to continue providing services.

Mrs. Melissa Staff, Sentinel's Senior Vice President of Field Operations, is responsible for the management and oversight of our Regional Account Management team as well as Sentinel's national network of customer support and branch office personnel. Her team manages the day-to-day needs of our benchmark offender-funded programs as well as providing customer service to our agency-funded contracts across the United States. **A dedicated account representative will be assigned to each Participating Agency for the duration of contract operations.** The Sentinel account representative will be responsible for:

- + Account retention;
 - + Being the main liaison between the Customer and Sentinel;
 - + Providing consultative account management practices to government channel accounts in their region to ensure best practices are in place;
 - + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
 - + Introduction and socialization of hardware and software offerings that may benefit the Customer;
 - + Conducting training and overseeing the implementation; and
 - + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.
- The Contractor must provide support functions 24/7/365.

SENTINEL RESPONSE

Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained technicians and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

Our monitoring centers are staffed 24 hours a day, 7 days a week with live staff including a supervisor always on duty and certified operators cross-trained to support our suite of supervision services and monitoring products. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, seven (7) days a week, 365 days a year. **There is no subcontracting of any of our proposed monitoring services.**

Sentinel provides access to designated **Help Desk** staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. Sentinel provides toll-free telephone access, toll-free fax line, and email access to over 60 operators and customer service representatives, available to officers 24 hours a day, 7



days a week, 365 days a year, who can resolve most technical problems over the telephone or through remote diagnostics.

Sentinel strives to resolve all customer inquiries promptly and on first contact. Each monitoring center operator has the expertise to easily identify, explain, and resolve issues relating to customer needs such as equipment installations, performing participant enrollments/terminations or entering/modifying data into the system, interpreting and/or clearing an alert and changing a participant's schedule.

In addition, this specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

- The Contractor must provide toll free access to customer support/monitoring center.

SENTINEL RESPONSE

As stated above, Sentinel provides toll-free telephone access, email access, and toll-free fax line access to highly trained operators and customer service representatives assigned to our Help Desk and National Monitoring Centers. These representatives are available to officers 24 hours a day, 7 days a week and can assist with the resolution of technical issues telephonically or through remote diagnostics.

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

In the unlikely event that problem solving requires a higher-level of involvement, Sentinel's customer service is equipped with all necessary computer equipment and staffed by experienced technicians, as well as the engineers who developed the system technology, who can quickly analyze and resolve the problem.

- The Contractor must provide initial start-up training that must include but not be limited to the following:
 - o The enrollment of clients into the software system.
 - o The installation, use, de-installation, and cleaning of the equipment.
 - o The generation and interpretation of data/monitoring reports.
 - o Accessing/using Contractor's technical support/help menus and monitoring center.

SENTINEL RESPONSE

Sentinel understands that training and customer service are crucial to the success of any electronic monitoring program, and Sentinel is dedicated to meeting those needs. Sentinel agrees to provide the initial training session and ongoing training, including all manuals, concerning the implementation and management of the monitoring



program as determined by the contract. Sentinel is committed to establishing a partnership over the term of the contract to ensure that all staff members are fully and properly trained. Training is offered for the life of the program as outlined in the monitoring services agreement at no additional cost.

Sentinel's training philosophy for our instructor-led courses can be a combination of respondent training as well as train-the-trainer if so desired by the Participating Entity. We work to provide all training for our customers based on their individual programmatic needs and thus will work with the Participating Entity to develop and deliver a training format that provides the best solution for each training location. Sentinel's standard training minimally includes the following items: installation and de-installation of equipment; maintenance and cleaning of equipment; use of web-based information system including procedures for enrollment and curfew changes as well as the generation and interpretation of reports; troubleshooting monitoring problems; accessing our technical support and monitoring center; and any additional training as needed to remain current on monitoring equipment and web-based information system.

Sentinel's implementation team will train all agency personnel assigned to the program prior to deployment and as needed for changes to the system, equipment, web-based information system, or personnel, for the duration of the program as directed by the contract. Our standard training protocol includes demonstration, discussion, and hands-on sessions on the following topics:

- + All RF, GPS, Alcohol Monitoring equipment, and client app solutions (use, installation, removal, and troubleshooting)
- + Enrollment (enrollment, deactivation, and the setting of all monitoring parameters including curfew schedules and GPS zones)
- + Tracking and monitoring of participants
- + Alarm processes and resolution procedures (agency-specific protocols)
- + Notification processes and reports (agency-specific protocols)
- + Monitoring System (complete instruction on the use of the web-based information system including, but not limited to, participant enrollment, modifications, reports, schedules, advanced automated analytics, location review, and deactivations)
- + Interpretation of Monitoring Reports (review, define and interpret daily monitoring activity, and Glossary of Terms/definitions)
- + Mobile Application (complete instruction on the use of the Mobile App including, but not limited to, participant information modifications, schedules, location review, device command initiation, field contacts, equipment inventory, and reports/activity review)
- + Accessing Technical Support and Help Desk Services (contact information and access to training support materials)

- The Contractor must provide materials and brochures on the use of the equipment and system.

SENTINEL RESPONSE

Sentinel will provide all user guides, user manuals, brochures, PowerPoint presentations, reference guides, and training videos on the use of the equipment and system for each Participating Entity. Additionally, Sentinel will provide instruction and hand-out material for agency staff to instruct program participants on the use, care, and charging of the equipment.



- The Contractor must provide on-going and supplemental training offerings either on-site or via web-based programs at a minimum of once (1) per year after the initial start-up training offerings or on an as needed basis, based on any significant changes to the Contractor provided equipment and/or technology.

SENTINEL RESPONSE

In addition to the initial training and set up process with a representative on location, the Sentinel Training Department offers either on-site or via webinar training sessions for customers and staff at a minimum of once (1) per year after the initial start-up training offerings, on an as-needed basis, or based on any significant changes to equipment and/or technology. This training is offered for all technologies and services including those proposed herein. It is important to note that Sentinel's webinar training sessions involve interactive voice plus visual contact with a live Sentinel expert trainer, therefore trainees can ask questions and engage in discussion with the trainer as part of any webinar.

Training and webinars are offered at no additional cost to the Participating Entity based on internal training calendars, individual training needs, and scheduled on demand. Webinars are conducted based on contract specifications and/or training needs and can include training on equipment, services, software, web-based system changes, and/or updates. Training is offered for the life of the program as outlined in the Master Agreement. At any time, a Participating Entity can contact our Help Desk for additional support to ensure they are maximizing the technology solution to its fullest potential.

Remaining Category 3: Alcohol Monitoring Questions

2. Describe the hardware you propose to meet the requirements of the SOW, including battery life.

SENTINEL RESPONSE

SCRAM™ - SECURE CONTINUOUS REMOTE ALCOHOL MONITORING - SOLUTION

The SCRAM CAM (Continuous Alcohol Monitoring) device provides 24/7 alcohol monitoring for higher-risk/higher-need alcohol clients. It is the most widely used and the only scientifically proven and court validated device of its kind. Additionally, SCRAM CAM boasts an impressive battery life of 90+ days, significantly reducing the need for constant communication and supervision. The bracelet uses a Lithium CR2, disposable battery with a 90-day life in use. No charging by the client is required. The bracelet will post a low battery message seven days prior to battery failure, allowing enough time for the battery to be replaced.



Designed specifically for alcohol monitoring programs where abstinence is required and house arrest may also be needed, SCRAM CAM provides supervising authorities with a fact-based, comprehensive profile of higher-risk clients' alcohol consumption and curfew compliance. The result is a much more reliable and cost-effective alternative to random breath testing or incarceration, making it an intensive accountability tool. The SCRAM CAM solution:

- + Encourages compliance because it eliminates testing gaps—meaning that there is no way to miss a test or drink around testing schedules.
- + Never requires a secondary test, such as a breath or blood test, to confirm a drinking event.
- + Is independently tested and has peer-reviewed, published studies confirming its reliability.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Is court-validated—meaning that it has been upheld as valid and reliable by the Daubert, Frye, and FRE 702 and 703 standards of admissibility in every state where it's been challenged.
- + Uses a controlled, quantifiable sample, resulting in true continuous monitoring and the lowest false positive rate possible. Competing devices do not use this testing protocol, making their devices simply sensors that are susceptible to environmental factors causing false positives and/or may require a secondary test.
- + It is the only system with a thorough record of independent testing and court admissibility.
- + Delivers 99.3% average daily compliance rate, proving SCRAM CAM's reliability and ability to deter drinking.
- + Uses a controlled, quantifiable sample, resulting in true continuous monitoring and the lowest false positive rate possible.
- + Still the most widely used product of its kind in the world, used to monitor over 700,000 clients since product release.
- + Equipped with industry-leading, anti-tamper technology that incorporates multiple sensors and accurately detects any tamper attempts.
- + Has a 90-day battery life in use. No charging by the client is required.

The SCRAM CAM Components: The SCRAM CAM bracelet is an ankle-worn transdermal device that is 2.8" long by 2.8" wide by 0.75" high and weighs only 5.8 oz. The base station is 6" long by 6" wide by 3" high and weighs 15 oz. The SCRAM CAM Bracelet is equipped with a disposable battery capable of being replaced in the field. This battery lasts 90 days once in use. A Battery Low alert generates when the battery voltage has become low, and an automatic "change battery" event will generate as a warning 60 days from installation. Additionally, the base station is equipped with a 48-hour backup battery and nonvolatile memory.

Sentinel offers *landline, cellular/Wi-Fi, and ethernet-based base stations / receivers* for use with the SCRAM CAM bracelet. Additionally, the SCRAM CAM unit is the only transdermal unit that can function without the need for a base station or a residential telephone line. Through its Direct Connect computer access, results can be downloaded via laptop or desktop computer by authorized personnel at any location, at any time. Please see below for further details of the base station and Direct Connect device.

- + **SCRAM CAM Bracelet:** The patented SCRAM CAM ankle bracelet transmitter is attached to the participant with a durable tamper alert strap. It is worn 24/7 by the program participant and captures transdermal alcohol readings by sampling the insensible perspiration collected from the air above the skin. For comfort purposes, the ankle strap is hypoallergenic. The bracelet transmits data via a wireless radio frequency (RF) signal to the SCRAM CAM base station. In addition, the SCRAM CAM system has optional house arrest capabilities, allowing it to monitor the wearer's presence or absence within the participant's home.
- + **SCRAM CAM Base Station:** The SCRAM CAM base station is the mechanism by which the data that is collected by the SCRAM CAM bracelet is transmitted for analysis and reporting to the SCRA Optix system. When the SCRAM CAM bracelet is installed on the participant's ankle, the program participant also receives the SCRAM CAM base station, which plugs into an analog telephone line, usually in the participant's home or place of work or to an Ethernet connection; a cellular-enabled version is also available for participants who do not have residential telephones or Ethernet connection.



The range between the base station and the bracelet can be set to "Minimum," "Average," or "Maximum" to account for the size of the client's home or other authorized location. These settings are approximately 35, 75,



and 150 feet, respectively. The SCRAM CAM base station includes an LED indicator and an audible alarm that can be enabled to alert the client when they are out of range. The SCRAM CAM base station can hold up to a month's worth of data (about 7500 messages). This equates to about 48 tests per day, or 1,440 tests per month. All messages are time-stamped and stored in its non-volatile memory, so that the messages are never lost.

The SCRAM CAM base station is optimized to communicate by standard telephone line or the Internet using the Ethernet port, as well as Wi-Fi and cellular connectivity. The bracelet communicates all alerts with the base station when in range, which then sends all available data to the monitoring system. At a pre-scheduled time(s) each day, the SCRAM CAM bracelet "communicates" with the base station, which then retrieves all available data from the bracelet and sends it for review. The base station also downloads monitoring and reporting schedules to the bracelet. Additionally, the SCRAM CAM base station is available with **Ethernet connectivity** to allow the unit to communicate over the internet using the participant's home modem. The Ethernet port at the back of the base station connects to almost all modems, regardless of internet service provider. Ethernet connectivity is a modern alternative to landline communication.

- + **SCRAM CAM Direct Connect:** In cases where a program participant may be required to report to agency personnel on a weekly basis, he or she can come into the supervising authority's office to have data that has been stored in the bracelet downloaded via the SCRAM CAM Direct Connect device. The compact Direct Connect device is slipped over the participant's bracelet (while worn) and attached by USB cable to an internet-enabled computer. The stored information is then transmitted from the SCRAM CAM bracelet directly for review without the need for a base station.

Tamper Resistant Features: The SCRAM CAM unit attaches to the participant's ankle using a secure strap and locking system and has built-in alarm technology that detects any attempt to tamper with the device. The SCRAM CAM bracelet is equipped with industry-leading, anti-tamper technology that features sensors to detect and report attempted tampers. These sensors determine whether the bracelet has been cut, removed, obstructed, or displaced. The bracelet's intelligent self-diagnostic capabilities constantly monitor and report its functionality. The SCRAM CAM device also has a built-in infra-red sensor on the inner part of the device itself. If the participant attempts to wedge any foreign matter between the device and his/her ankle, the infra-red sensor will detect the attempted intrusion of the foreign object and trigger an alert. This design allows the device to utilize multiple tamper detection methods to ensure program integrity. **Any attempts to tamper with the bracelet or its functionality will be immediately detected by the SCRAM CAM system.**

Alcohol Testing Protocols: SCRAM CAM tests for alcohol consumption by measuring the concentration of ingested alcohol present in the insensible perspiration that is constantly produced by the skin. SCRAM CAM automatically collects these samples of perspiration from the air above the participant's skin and transmits this data to a central source for analysis – requiring no effort on the part of the program participant or the supervising agency. Because people excrete approximately one percent (1%) of the alcohol they drink through their sweat, if an individual has been drinking it shows up in the level of ethanol vapor present in this insensible perspiration.

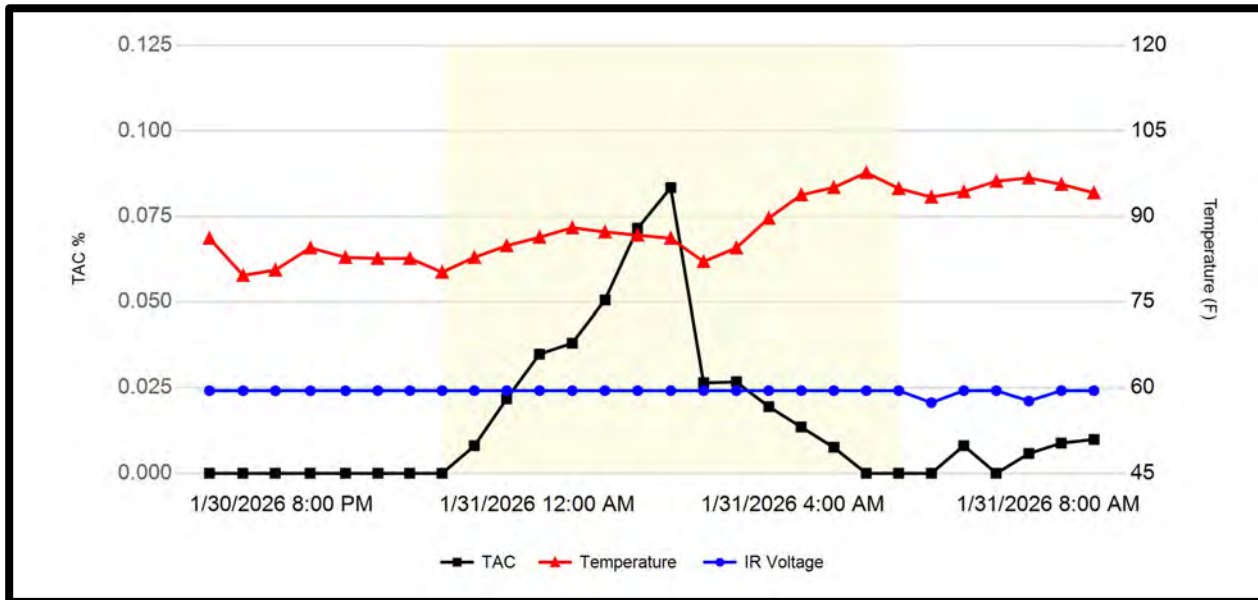
All data received from the SCRAM CAM bracelet is subjected to a rigorous, scientific alcohol detection analysis. This review process, supervised by SCRAM Systems' specially trained team of analysts, looks at key data (such as alcohol absorption and elimination rates) of the Transdermal Alcohol Content (TAC) curve. This peer-reviewed, scientifically proven, and court-validated confirmation process ensures that only true alcohol consumption events are confirmed.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SCRAM CAM readings and analysis are based on the well-documented and scientifically proven metabolism rate for consumed alcohol. Data from a drinking event shows a gradual increase in alcohol levels over time, achieves a maximum TAC, and then slowly burns off to create a well-defined alcohol curve. In the following graph, TAC is represented by the black line. Tamper detections, in the form of an infrared (IR) sensor (represented by the blue line) and temperature reading (represented by the red line) appear on the graph along with the TAC readings.



This ensures that alert notifications are reliably confirmed as valid so that no additional follow-up testing or examinations, such as blood, breath, or urine, are necessary to confirm drinking events. The system can distinguish between alcohol consumption and environmental or interfering alcohol-based products, such as lotion, cologne, and spilled alcohol, thereby eliminating false alerts. All confirmed violations are automatically date- and time-stamped, sent to agency supervising authorities by 9:00 a.m. the following day via the communications method and medium chosen by the agency. **A Daily Action Plan (DAP) typically delivered via email every day shows which participants had specific violations.**

Unique Features of the SCRAM CAM Solution: The following are highlights on the SCRAM CAM transdermal alcohol monitoring device:

- + Measures the concentration of alcohol in the blood through the skin providing a Transdermal Alcohol Concentration—or TAC—reading;
- + Requires no involvement or scheduling by the participant, thereby ensuring regular and accurate testing;
- + Eliminates testing gaps and provides 24/7 coverage, so participants cannot drink around test schedules;
- + Can withstand changes in temperature and humidity without generating a false positive;
- + Does not require a secondary test, such as a breath or blood test administered by a field officer, to confirm a drinking event;
- + Is independently tested and has national peer-reviewed, published studies confirming its reliability;
- + Includes a comprehensive court support program where the manufacturer will testify in court concerning the technology and specific test results; and
- + Can prove reliably, in a court of law per the Daubert standard, and has been upheld as valid and reliable by the Daubert, Frye, and FRE 702 and 703 standards of admissibility in every state where it has been used to monitor participants.



SCRAM CAM continues to be validated in court hearings across the country. To date, a SCRAM Systems expert witness has participated in 130 evidentiary-level hearings in 24 states, with 33 of the Hearings resulting in a Frye, Daubert, or hybrid ruling. As part of the 130 hearings, three State Supreme and Appellate Court rulings have been made in favor of SCRAM CAM and subsequent monitoring results.

—IMPORTANT SENTINEL ADVANTAGE—

Feature Release | Next-Generation Alcohol Monitoring. Upon release, the new SCRAM CAM Connect will provide wireless alcohol monitoring with built-in GPS and Wi-Fi geolocation without the use of a base station. Features of the SCRAM CAM Connect include:



- + **Compact and Comfortable Design.** Smaller, lighter, and thinner devices support both punitive and non-punitive usage. The hypoallergenic, compact form enhances comfort and reduces stigma for clients.
- + **Enhanced Connectivity.** Provides more communication options through Cellular and Wi-Fi, eliminating the requirement for a separate base station.
- + **Timely Notifications and Alerts.** Enables immediate notifications regarding potential drinking, tampering, or device removal events, including real-time location updates.
- + **Location Monitoring Services.** Offers GPS, Wi-Fi geolocation, and cellular triangulation for flexible tracking solutions.
- + **Extended Battery Life.** Features a 90-day battery cycle to minimize maintenance and interruptions.
- + **Optional Field Calibration Support.** Specifically optimized for voluntary sobriety and treatment populations, allowing for tailored monitoring strategies.
- + **Flexible Service Modes.** Available in three service options, SCRAM CAM Connect offers Wi-Fi only, SCRAM CAM 360 adds a cellular communication option, and SCRAM CAM Plus location monitoring, to meet diverse client needs.

SCRAM™ REMOTE BREATH® PRO ALCOHOL MONITORING SOLUTION

The SCRAM Remote Breath Pro is a portable wireless breath alcohol monitoring device that provides a GPS location with both taken and missed tests. The device communicates via cellular networks and notifies supervising authorities of any alcohol readings (BrAC), tamper alerts, or possible equipment malfunctions so they can quickly respond. Remote Breath Pro is powered by a rechargeable Lithium-Ion battery. The device typically lasts two (2) days in between charges. The client is alerted by light indicators, text message, and/or audible alarm when the battery is low. The Remote Breath Pro offers the following features and benefits:

- + Sleek, lightweight, and compact. The device measures 2.9"x6.5" with a 1.2" depth.
- + Facial authentication decreases officer photo manual matching by up to 95%, allowing officers more time to spend on their caseloads and participants.
- + Enhanced facial guidance provides visual cues ensuring face is aligned during participant testing
- + Device-initiated testing—automatically turns on and prompts participants for scheduled and on-demand tests.
- + Wi-Fi capability so that downloads can be performed when a cellular connection is not available.
- + Store and Forward—never lose test results.
- + GPS location with both taken and missed tests.

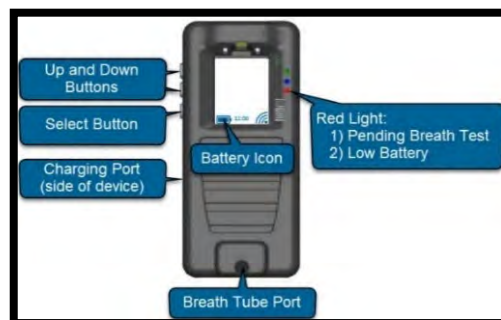
**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



User-Friendly Design. The handheld device is sleek, lightweight, and compact, weighing only 9.95 ounces. The device measures 2.9" x 6.5" with a 1.2" depth. The small and durable device comes with a fitted protective carrying case and adapts to the participant's everyday life, enabling participants to take a test anytime, anywhere.

The device is easy and simple to use, with clear instructions on the display screen and side-buttons to scroll up or down and select menu options. Participants can also adjust the volume and screen brightness as preferred.



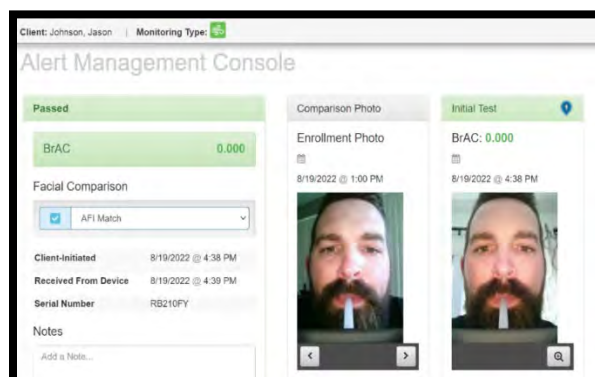
Rugged Design. The Remote Breath Pro is a rugged device built for corrections and not the general public. It has been subjected to rigorous drop testing and meets military drop test standards ML-STD810G, which means that it is able to operate after 26 drops on all edges, surfaces, and corners from four feet in height onto a two-inch plywood board over a concrete surface. The device is FCC certified (FCC ID P8M-AMSCGJMW1) and meets industry level ISO certification.

Enhanced Facial Guidance. The device provides visual clues ensuring that the participant's face is aligned during testing. The device will prompt the participant to first align their face, showing a red border, and then when ready, the screen changes to indicate that the participant should blow, showing a green border. This helps the participant take successful tests, increases participant compliance, and reduces the need for multiple tests.



Participant Feedback. The device also gives feedback to the participant during the enrollment and testing process to help ensure quality enrollment and testing photos. This feedback reminds participants to avoid sitting/not standing straight, direct sunlight, obstructions to the face, or holding the unit at an extreme angle (the breath tube must be level). This functionality allows the user to correct these factors with an immediate retest, resulting in an increased likelihood of a match—saving time and money by reducing the need for officers to manually match photos. Poor tests are corrected in real-time with onboard processing.

Automated Facial Intelligence (AFI). The device captures participant images with a 5-megapixel, high-resolution camera and the AFI system uses facial matching to automatically examine and compare the images. AFI is the same facial authentication technology used internationally by government security forces. The system automatically scans and confirms the participant's identity with each breath test to eliminate manual matching of photos by up to 95%. Facial matching technology eliminates the need to scroll through numerous photos, increasing accuracy and efficiency, and reducing risk. It enables real-time notifications when the participant does not match and allows the officer to immediately address a potential violation.

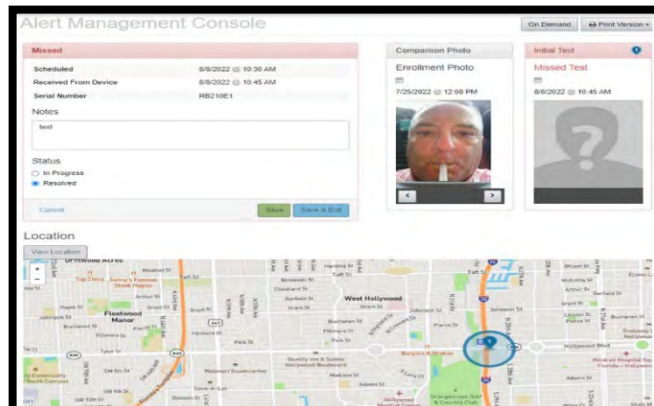


**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



The Remote Breath Pro device automatically powers itself up during test windows and tracks its location at the time of the scheduled test. The device provides a GPS location with every test—both taken and missed tests. A GPS location with a missed test is especially useful as it can help an officer make a more informed decision as to why a participant missed a test. For example, participants often state they missed a test because they left their device at another location. Officers can verify or refute the participant's claim by comparing the GPS point on a missed test (verified via GPS ping) with the participant's location.



Proven Electrochemical Fuel Cell Technology. The electrochemical fuel cell used in the Remote Breath Pro has been validated through decades of research and experience. It is considered the most reliable in alcohol testing applications. This is the same fuel cell used in evidential breath testing and interlock devices and consists of extremely sensitive ethanol-specific alcohol sensors.

Cellular Communication. The Remote Breath Pro uses the LTE AT&T network. The device uses a cellular modem that is supported by both 4G and 5G networks.

Wi-Fi Capabilities. The Remote Breath Pro has been enhanced to have Wi-Fi capabilities, so that participants without cell coverage can use home or public Wi-Fi to transmit test results.

Device-Initiated Testing. Because Remote Breath Pro stores the participant's test schedule on the device, it automatically turns on and prompts participants for scheduled and on-demand tests—even when out of cell coverage. Notification for both BrAC and positive participant ID is immediate.

Courtesy Reminders. Officers have the option to schedule reminders to be sent via text message to the participant's cell phone shortly before or at the test time. Text messages can also be sent for "Battery Low" and "Battery Critically Low" alerts to help the participant avoid a power fail situation and prevent unnecessary alerts to the officer. The automated courtesy reminders can be sent in English or Spanish.

Store and Forward. Competing breath devices rely on cell phone text messages to remind participants to test, but these devices cannot store test results when in an area without cell coverage. As a result, participants using these devices may miss tests simply because they are in an area with poor coverage. In contrast, the Remote Breath Pro incorporates a "Store & Forward" feature, which ensures a test is never missed. Its memory can store up to 48,000 test results when participants are out of cell service. The time-stamped results are forwarded as soon as coverage is regained.

Rechargeable Battery. The Remote Breath Pro is powered by a rechargeable Lithium-Ion battery. The device typically lasts 2 days in between charges. The participant is alerted by light indicators, text message, and/or audible alarm when the battery is low.

Request for Proposals for
ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Easy to Charge. The device is easily charged using modern and simple charging methods. It has a USB-C charging port and comes with a USB cable and adapter. Participants can connect the device to the included adapter and plug it into any standard wall outlet or simply charge it with a USB port using the supplied USB cable. A log is created in the information system showing a date and time stamped list of every time the device is charged. Officers can see the participant's specific charging patterns and tell how long a device was plugged in to determine if the participant is charging the device on a regular basis.

SCRAM [®] Remote Breath Battery Charge Summary					
8/29/2022 thru 9/15/2022					
Client:	Smith, Jillian		Caseload:	Adams County	
Case Number:	CA-2022-13-7-RB		Agent:	Miller, Phil	
Date of Birth:	1/17/1970		Court:	Douglas County Court	
			Judge:	Anderson, Judge	
Event	Plug In Time	Un Plug Time	Charge Time (dd:hh:mm:ss)	Reached Full Charge	
Plug In	8/31/2022 8:51 AM	8/31/2022 1:00 PM	0:04:09:14	Yes	
Plug In	9/2/2022 8:44 PM	9/6/2022 8:02 AM	3:11:18:16	Yes	
Plug In	9/8/2022 7:45 AM	9/8/2022 7:56 AM	0:00:10:47		
Plug In	9/8/2022 7:59 AM	9/8/2022 10:49 AM	0:02:49:47	Yes	
Plug In	9/8/2022 2:32 PM	9/9/2022 8:28 AM	0:17:55:20	Yes	
Plug In	9/12/2022 11:15 AM	9/13/2022 7:54 AM	0:20:38:37	Yes	
Plug In	9/15/2022 5:36 AM	9/15/2022 10:54 AM	0:05:18:16	Yes	

Tampering. The Remote Breath Pro ensures accuracy by using security-grade facial authentication to detect attempts to circumvent the system. The system automatically scans and confirms each participant's identity with each breath test. In addition, if the battery case is opened, a Device Housing Breach alert will be generated. Attempts to tamper or circumvent the system will be reported per predefined Agency procedures.

SHADOWTRACK SHADOWBRIETY (OPTIONAL)

Sentinel is proposing, **as an option**, the Shadowtrack ShadowBriety, a portable handheld remote breath alcohol monitoring device that is paired with a participant's smartphone through Bluetooth technology. The ShadowBriety solution incorporates advanced facial recognition and an electro-chemical fuel cell technology to provide actual quantitative BAC readings. Highlights of the unit include:

- + Provides sobriety testing through the inclusion of the ShadowBriety BACtrack Portable Breath Alcohol Testing Device
- + Through facial recognition and Bluetooth technology, results are immediate, accurate, and specific to the participant
- + Captures the participant's BAC level along with a GPS location of each test
- + Communicates via cellular networks and/or available Wi-Fi services
- + Test schedule options include random, fixed time, and on demand
- + Results Documented within the Monitoring Application
- + Frequency Determined by Officer
- + caseload/dashboard
- + Caseload Management Integration
- + Anti-Spoofing Technology Built In



User-Friendly Design. ShadowBriety alcohol Monitoring solution includes the BACtrack remote alcohol monitoring device that lightweight, discreet, and easy to use, measuring 1.75 x 2.75 x 0.63 inches and weighing 1.75 oz. and provides test notifications through push technology or SMS.

Rechargeable Battery. ShadowBriety is powered by a Li-Ion battery that provides over 5 days of operation and is Rechargeable with the included micro-USB cable.

Rugged Design. The ShadowBriety - BACtrack alcohol devices are designed to be rugged and reliable, provide high accuracy and compliance with professional standards. They are compact and portable, making them easy to

Request for Proposals for ELECTRONIC MONITORING

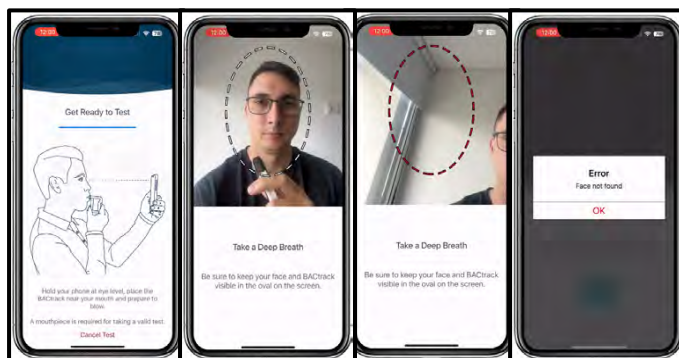
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



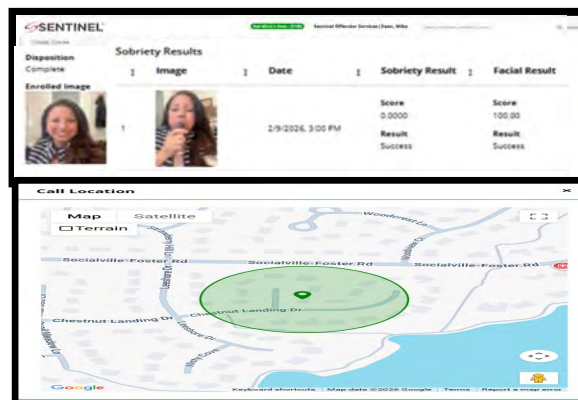
carry and use on the go. The ShadowBriety - BACtrack device is designed for various environments including law enforcement use. The device is FCC certified (FCC ID S8B-M5).

ShadowBriety has undergone rigorous testing standards to ensure the ShadowBriety is a reliable and trustworthy device for monitoring alcohol concentration and incorporates the following technologies to ensure reliability and accurate testing.

Enhanced Biometric technology. ShadowBriety uses advanced facial detection technology to verify that a visible face is present, if No face detected, or if Tester is not facing forward, and the test is being blocked. These features are designed to prevent tampering; the test also stops if it detects more than one face in order to keep every test honest by requiring the tester to show their face and preventing multiple faces on-screen. It also incorporates advanced features that confirm the participant is blowing into the breath tube securely attached to the ShadowBriety - BACtrack device.



Automated Facial Recognition Technology & Location Based Monitoring Technology. ShadowBriety captures participant images with high-resolution camera and uses facial recognition technology to verify the program participant at time of testing to verify identity during each test, ensuring that the facial results are reliable and court admissible. The system automatically scans and confirms the participant's identity with each breath test to eliminate manual matching of photos. This process eliminates the need for an officer to scroll through numerous photos, increasing accuracy and efficiency, and reducing risk. It enables real-time notifications when the participant does not match and allows the officer to immediately address a potential violation.



Proven Electrochemical Fuel Cell Technology. The electrochemical fuel cell used in ShadowBriety accuracy was validated against police testers in a study published in the Journal of Injury Prevention, demonstrating its reliability. This is the same technology trusted by police and professionals for accurate screening.

Cellular & Wi-Fi Communication. ShadowBriety uses the LTE network for communications and has enhanced Wi-Fi communication capabilities.

Random, Pre-Set, and On-Demand Testing. Officers have the flexibility to set up alcohol test schedules based on the individual need on a case-by-case basis.

Communication & Courtesy Reminders. Officers have the option to schedule reminders to be sent via text message to the participant's cell phone shortly before or at the test time. The automated courtesy reminders can be sent in English or Spanish. Officers can also have program participant to Check in at Random or Pre-set Times to confirm Locations, during times an alcohol test is not required.

Rechargeable Battery. The ShadowSobriety - BACtrack Mobile is powered by a rechargeable Lithium-Ion battery. The device typically lasts 5 days in between charges. The participant is alerted by light indicators, text



message, and/or at the time they are taking a test when the battery is low.

3. Describe your software system (web-based applications, smart phone applications).
Describe unique design features that ensure accuracy and/or speed of reporting.

SENTINEL RESPONSE

SCRAM SYSTEMS WEB-BASED SOFTWARE SYSTEM

SCRAM Optix is a comprehensive, secure, and fully integrated supervision technology platform designed to support alcohol monitoring, location monitoring, and client engagement through both web-based applications and smartphone-based applications. These applications operate together to provide real-time data visibility, improve officer efficiency, and ensure the accuracy and timeliness of monitoring information. SCRAM Optix is secure, scalable, and accessible 24/7 via any web-enabled device. Officers can enroll clients, adjust device settings, enter/edit schedules, select notification methods or parameters, manage inventory and quickly access detailed caseload information at-a-glance via device and status indicators. It offers robust caseload and client management tools, including both point-by-point and advanced mapping with pattern of life features, inclusion/exclusion zone management, customizable notification protocols, and powerful program reporting tools.

Since mobile applications often have limited functionality, SCRAM Optix is designed to be mobile-adaptive, allowing users to access all features available on a computer or from a smartphone or tablet. Adaptive design can help ensure faster page load speeds and consistent user experience across different screen sizes. It requires no

SCRAM Optix monitoring program reports offer unprecedented options to acquire, store, analyze, evaluate, and convert raw data into valuable information—such as compliance rates and average monitoring periods, as well as behavioral trends based on age, gender, severity of offense, and duration of monitoring. Unique data visualization provides quantitative and qualitative views along with powerful reporting that delivers instant access to program performance. Flexible templates deliver visual Key Performance Indicators (KPIs) for commonly accessed program performance metrics such as: compliance by officer, alert analysis, and breakdown by device, client, and courts. This unparalleled insight into an agency's program is easily accessed and intuitively queried so program efficacy can always be measured.

- + **Alert Analysis Report.** This report provides a graphical breakdown of alerts that can be displayed by device monitoring type for the previous month, quarter, or year providing officers with an efficient, time-saving tool by which to compare percentage of clients with violations as opposed to violations generated overall. Alert information is broken down by day of the week and each month of the year to help analyze client trends.
- + **Client Breakdown Report.** This provides a graphical breakdown of clients by offense type, client type, and referring court displaying data for completed clients monitored by offense or offender type, or specific court, during the time period specified. Each monitoring type displays the total clients monitored, average monitoring days, compliance percentage, and average days to the first violation over the last month, quarter, or year.
- + **Client Compliance Report.** This report shows daily compliance percentage per equipment type, providing number of clients monitored, amount of violations by type, and average number of monitoring days. The report can be displayed by week, month, or year. Officers can accurately assess program needs and compare individual program statistics to the national average by product types.

UNIQUE DESIGN FEATURES ENSURING ACCURACY AND SPEED OF REPORTING FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM alcohol monitoring solutions include multiple device-level, software-level, and workflow-level design features that enhance data accuracy and support rapid reporting.



- + SCRAM CAM provides scientifically validated, court-admissible continuous alcohol monitoring by sampling insensible perspiration every 30 minutes. It includes advanced anti-tamper technology such as strap integrity detection, obstruction monitoring, and supplemental environmental indicators. Multi-path communication options—including RF, Ethernet, Wi-Fi, and cellular—ensure monitoring data is transmitted quickly and reliably. The system generates immediate alerts for alcohol detection, tamper events, and equipment issues, allowing supervising authorities to respond without delay. Officers have access to comprehensive reporting tools, including longitudinal activity summaries, compliance charts, and detailed event histories.
- + SCRAM Remote Breath Pro ensures accuracy through high-resolution facial authentication that compares each test image to an enrollment baseline. The device also applies location tracking to both completed and missed tests, giving supervisors accurate contextual information for compliance verification. Real-time, on-device user prompts improve test quality and reduce invalid submissions. Cellular and Ethernet connectivity ensure rapid data transmission, while automated test initiation and immediate alerting enable fast supervisory action.

SYSTEM-WIDE ACCURACY AND REPORTING PERFORMANCE FEATURES FOR SCRAM CAM AND REMOTE BREATH PRO

Across all SCRAM monitoring technologies, the following system-wide features enhance performance:

- + **Consolidated Alert Management.** High-priority events—including alcohol use, tampers, location violations, and missed tests—are elevated in the monitoring dashboard to ensure rapid response.
- + **Mobile-Adaptive Officer Access.** Officers can access caseloads, alerts, participant profiles, schedules, and device status from smartphones or tablets, supporting timely decision-making in the field.
- + **Advanced Reporting and Analytics.** The system includes comprehensive reporting tools and analytics that provide insights into compliance trends, alert patterns, monitoring durations, and participant behavior. These tools allow agencies to identify issues quickly and respond efficiently.
- + **Configurable Notification Protocols.** Agencies may tailor alert recipients, notification types, escalation levels, and distribution rules to ensure the right personnel receive information as quickly as possible.

SCRAM Optix ensures accurate, reliable, and timely reporting for alcohol and location monitoring programs. Its combination of validated monitoring technologies, biometric verification, GPS tracking, advanced tamper detection, real-time alerts, and mobile-adaptive supervisory tools provides a comprehensive solution that fully meets the requirements for accuracy and speed of reporting.

SMARTPHONE APPLICATIONS FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM TOUCHPOINT

SCRAM TouchPoint is a participant-facing smartphone-based application that enhances monitoring efficiency and participant accountability when used alongside the SCRAM CAM and SCRAM Remote Breath Pro equipment. The following outlines the functional scope of services provided through this integration.

- + **Automated Electronic Monitoring Reminders.** SCRAM TouchPoint supports SCRAM CAM and SCRAM Remote Breath Pro through automated notifications that improve participant compliance and reduce preventable violations. These reminders include, but are not limited to:
 - o Device charging requirements
 - o Routine equipment maintenance
 - o Prompts to contact supervising officers
 - o Scheduled or required monitoring actions

All reminders are delivered directly to the participant's smartphone and include confirmation receipts visible to supervising officers.



- + **Participant Compliance Support.** The system reduces administrative workload by ensuring participants receive consistent, automated guidance regarding their CAM or Remote Breath Pro equipment. Benefits include:

- Fewer missed tests and avoidable alerts
- Increased adherence to supervision requirements
- More efficient case management for officers

This automated support improves reliability of program operations and enhances participant accountability.

- + **Integrated Communication Tools.** TouchPoint enhances monitoring programs through seamless communication features:

- Secure, two-way messaging between officers and participants
- Read receipts for all communication
- Ability to transmit documents, forms, and electronic signatures
- Automated notification layering (in-app + push alerts)

These tools strengthen participant engagement and reduce reliance on in-person interactions.

- + **Supplemental Monitoring Capabilities.** While SCRAM CAM and SCRAM Remote Breath Pro conduct alcohol monitoring independently, TouchPoint provides supplemental oversight tools that support program objectives:

- GPS-enabled check-ins with biometric and photo verification
- On-demand location confirmation
- Participant-submitted updates and status confirmations

These capabilities enhance compliance tracking without replacing core device functions.

SHADOWTRACK WEB-BASED MONITORING SOLUTION

The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with an agency's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing participant access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

Shadowtrack has a wide array of report options ranging from violation reports to inventory control that can be downloaded, printed, and/or exported in various formats. From within the monitoring platform, supervising personnel can easily review/download/print/export the activity of a single participant or generate additional reports specific to an agency's needs. Reports are available via various formats including PDF, Excel, etc.

- + Caseload at a Glance
- + Alcohol Monitoring Tests
- + Missed Test / Check in
- + Automated and Ad Hoc Reports
- + Event History
- + Multi-point client enrollment
- + Client deactivation



+ Analytics

The platform allows users to manage their caseload activity, enroll new participants, enable monitoring services, schedule monitoring services and events, view alcohol monitoring test results, test locations, and compliance history, generate custom reports, electronically communicate with the participants, and more. The Shadowtrack web-based monitoring application has several supervision modules that can be tailored to each user agency needs and requirements. Essential features include:

- + Reliable Remote Alcohol Monitoring
- + Smartphone Monitoring Solutions using their personal IOS or Android smartphone
- + Multi-Factor Authentication with facial recognition and voice verification
- + Location verification at the time of check-in/interview utilizing geofencing and individual participant scheduling
- + Smart Device Battery/Status transmitted with each check-in/interview
- + Officer Notification of missed check-ins, failed check-ins, enrollment completion, geofence violations
- + Appointment Reminder with push notifications and automatic updates to the participant's app calendar
- + Video Calling, SMS/Text Communication, In-App Chat, Voicemail Delivery
- + Scheduled weekly/bi-weekly/monthly Mobile Interview scheduling
- + Scheduled, self-initiated and on-demand participant Mobile Check-ins
- + Scheduled, self-initiated and on-demand participant location Requests

SHADOWTRACK SMARTPHONE APPLICATIONS

Shadowtrack's Officer Mobile applications and Web applications require secure authentication for access to data and utilize role-based access control to constrain access.

Shadowtrack's Officer Mobile App provides a mobile version of software that can be utilized as an officer mobile app. The software Application detects when an authorized user is accessing the software platform via a mobile device (cellphone/laptop/tablet, etc.) and will automatically adjust browser settings for that particular device including both Apple and Android platforms. All functionality within the software application can be customized as to what features are displayed. These features include but are not limited to the ability to view alcohol test results, view client test location points, caseload dashboard, case management notes, as well as the functionality to edit schedules.

4. Describe the alerts that can be set up (time, tamper alerts, positive result, low battery, etc.). Describe the process for setting system alerts for violations. Include the alert intervals and how long it will take for the hardware to communicate with the software. Describe how the technology reduces false tampers and ensures accurate alert notification.

SENTINEL RESPONSE

AVAILABLE ALERTS FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM CAM provides a comprehensive alerting framework that delivers timely, accurate notifications to support supervision, compliance, and program accountability. Alerts are automatically generated through continuous monitoring, device diagnostics, and communication checks, and are transmitted to the monitoring system for officer review.



- + **Alcohol Consumption Alerts.** SCRAM CAM continuously measures transdermal alcohol concentration and generates alerts when alcohol use is detected. The device's sampling method and analysis process ensure that only confirmed alcohol consumption events are reported, supporting accurate and defensible monitoring results.
- + **Tamper Alerts.** The device includes advanced, multi-sensor anti-tamper technology designed to detect any attempt to interfere with bracelet function. Alerts are generated for conditions such as.
 - o Attempts to remove, obstruct, or cut the bracelet
 - o Interruptions in skin contact
 - o Temperature irregularities associated with tampering
 - o Proximity tampering caused by foreign objects placed between the device and the skin
- + **Environmental Alcohol Alerts.** SCRAM CAM evaluates ambient air before every reading to distinguish environmental alcohol from consumed alcohol. The device generates alerts when environmental exposure is detected, helping officers determine whether the source of alcohol is environmental or ingestive.
- + **Low Battery Alerts.** SCRAM CAM features a long-life, 90-day disposable battery. The system issues a low-battery alert approximately one week before the battery is expected to expire, ensuring uninterrupted monitoring and timely maintenance.
- + **Communication and Base Station Alerts.** The system generates alerts when bracelet or base station communication is disrupted, including events such as.
 - o AC power interruptions and restorations
 - o Phone line or communication loss and restoration
 - o Base station movement (in programs using location verification)
 - o Out-of-range conditions when RF curfew monitoring is active
- + **House Arrest / Curfew Alerts (When RF Is Enabled).** When SCRAM CAM is configured with integrated RF monitoring, the system can generate curfew-related alerts, including:
 - o Curfew violations
 - o Range violations
 - o Unauthorized movement of the base station

SCRAM Remote Breath Pro provides a comprehensive alerting system that supports reliable, real-time monitoring of breath alcohol results, identity verification, device integrity, and compliance with scheduled testing. Alerts are automatically generated by the device and transmitted through the monitoring system for timely officer review and action.

- + **Alcohol Test Result Alerts.** The device performs BrAC testing using evidential-quality fuel cell technology and generates immediate alerts for any alcohol-positive result. Each alert includes the breath alcohol reading, identity verification, and GPS location. When a positive test occurs, the device can automatically prompt the participant for a confirmation test within a predetermined timeframe to validate the initial result.
- + **Facial Verification Alerts.** Every test includes automated facial authentication to verify the identity of the person taking the test. These alerts ensure testing integrity and significantly reduce instances of identity circumvention. Alerts are generated when:
 - o The face does not match the enrolled participant
 - o Identity verification cannot be completed
 - o A different individual attempts to take the test
 - o Obstructions, lighting issues, or improper positioning impact verification



- + **Tamper and Device Integrity Alerts.** SCRAM Remote Breath Pro includes tamper-resistant hardware and software features. These alerts help ensure compliance and allow immediate response to attempted manipulation. Alerts are triggered by:
 - o Opening or disturbance of the device housing or battery compartment
 - o Attempts to disable or bypass identity verification
 - o Any condition indicating potential interference with normal device operation
- + **Missed Test Alerts.** If the participant fails to complete a scheduled or on-demand test, the system generates a missed-test alert. Each missed test is accompanied by a GPS location captured at the scheduled testing time, allowing officers to compare reported whereabouts with verified device location.
- + **Low Battery and Critical Battery Alerts.** The device issues low-battery and critically low-battery alerts to both the participant and supervising officer. These alerts help prevent device shutdown, reduce avoidable missed tests, and support consistent adherence to monitoring protocols.
- + **Communication and Transmission Alerts.** Alerts are generated when the device is unable to transmit test results or data due to:
 - o Loss of cellular connectivity
 - o Interrupted transmission
 - o Failure to upload secured stored data

When coverage is restored, stored results automatically transmit, ensuring no test data is lost.

- + **Device-Initiated Testing Alerts.** Because test schedules are stored internally, SCRAM Remote Breath Pro automatically powers on to perform required tests. This ensures monitoring reliability even when the participant is temporarily outside cellular coverage. Alerts are generated when:
 - o Scheduled device-initiated tests are not completed
 - o Identity verification fails during device-initiated testing
 - o BrAC or identity issues arise immediately during the triggered test window
- + **Courtesy Notification Alerts.** Optional text reminders can be configured to notify participants shortly before scheduled tests. This feature enhances client success rates and reduces missed tests. These reminders may include:
 - o Upcoming test alerts
 - o Battery reminders
 - o General compliance-support notifications
- + **Alert Management Through Monitoring System.** Supervising officers can manage all SCRAM Remote Breath Pro alerts through the monitoring platform (SCRAM Optix), which allows them to:
 - o Review, resolve, and organize alerts by type, client, or caseload
 - o Access detailed event data including photographs, GPS points, and testing sequences
 - o Trigger on-demand tests in response to alert activity
 - o Prioritize urgent alerts and streamline exception-based supervision

SYSTEM ALERT CONFIGURATION AND VIOLATION NOTIFICATION FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM CAM and SCRAM Remote Breath Pro use standardized, defensible alerting processes designed to ensure accurate, timely, and verifiable notifications. Alerts are configured within the monitoring system to match agency requirements, with customizable delivery options and scientifically validated safeguards to ensure reliability.



SCRAM CAM | Configuring System Alerts

All alert settings—including drinking events, tamper events, environmental alcohol alerts, communication failures, curfew violations (when RF is enabled), and low-battery notifications—are configured through the monitoring platform. This allows agencies to tailor alerting to program needs while ensuring timely response to violations. Agencies designate:

- + Which alert types should trigger notification
- + Who receives each alert
- + The escalation sequence for critical alerts
- + Notification mode (email, text, or scheduled summary reports)

Alert Intervals and Communication Timing. SCRAM CAM continuously collects transdermal alcohol data. When the bracelet comes within communication range of the base station, it:

- + Transfers stored data immediately
- + Sends violation alerts as soon as the base station uploads the message to the software
- + Uses landline, cellular, Wi-Fi, or Ethernet connectivity to ensure rapid transfer

Power loss, phone line interference, environmental issues, and tamper-related events are time-stamped and transmitted automatically once communication is restored. Because test samples are collected every 30 minutes, violation-related alerts are generated as promptly as technology and communication allow.

SCRAM CAM | Reducing False Tamper & Ensuring Accurate Notifications.

SCRAM CAM employs multiple layers of anti-tamper validation:

- + Sensors that detect temperature shifts, loss of skin contact, strap or proximity interference
- + Automated ambient air sampling before every measurement to distinguish environmental alcohol from ingested alcohol
- + Scientific analysis of alcohol curves to validate true drinking events and rule out contamination
- + Self-diagnostic checks that continuously monitor device integrity

These combined safeguards drastically reduce false tamper reports and ensure that only accurate, verified alerts are sent to supervising authorities.

SCRAM REMOTE BREATH | Configuring System Alerts

Agencies configure alert rules for breath test violations, missed tests, identity mismatches, tamper conditions, communication interruptions, and battery-related issues through the monitoring platform. Options include:

- + Assigning alert recipients by role or caseload
- + Choosing between real-time notifications or grouped alert summaries
- + Setting thresholds for when positive tests trigger mandatory confirmation testing
- + Configuring random, scheduled, and on-demand testing windows and associated alerting

This flexibility enables agencies to align alerting protocols with program policy.

Alert Intervals and Communication Timing. SCRAM Remote Breath Pro is designed for real-time reporting:

- + Each test's BrAC, GPS point, and facial authentication result are transmitted immediately when cellular service is available
- + If the device is out of coverage, test results are stored with complete timestamps and forwarded automatically once service returns
- + Device-initiated test windows ensure the unit powers on and prompts testing even without coverage
- + Missed test alerts include a GPS location captured at the scheduled test time



These communication safeguards ensure prompt reporting without loss of test data.

SCRAM REMOTE BREATH PRO | Reducing False Tamperers & Ensuring Accurate Notifications

SCRAM Remote Breath Pro includes security-grade features to ensure reliability:

- + Advanced facial authentication prevents someone else from taking the test
- + High-resolution imaging and immediate on-screen user feedback reduce poor-quality or unverifiable photo captures
- + Device-housing breach detection alerts when the battery door or casing is disturbed
- + Fuel-cell alcohol detection ensures ethanol-specific test accuracy
- + Integrated GPS data validates the device's physical location for all tests, including missed tests

SHADOWTRACK SHADOWBRIETY ALERTS AND NOTIFICATIONS (OPTIONAL)

Notifications can be delivered via SMS text message, email, and/or via an automated voice call to a desired phone number(s). Additionally, field supervising staff can utilize Shadowtrack's Officer Mobile App and/or staff can utilize our desktop web-based monitoring software to monitor participants in real-time.

- + **Alcohol Test Result Alerts.** The ShadowBriety solution pairs a BACtrack Mobile Alcohol Monitoring device with a cell phone to perform highly accurate alcohol monitoring testing using evidential-quality fuel cell technology. The ShadowBriety system generates immediate alerts for any alcohol-positive result. Each alert includes breath alcohol reading, positive identify via facial recognition verification, and GPS location for where the test was taken. When a positive test occurs, the device can automatically prompt the participant for a confirmation test within a predetermined timeframe to validate the initial result.
- + **Facial Verification Alerts.** Every test includes automated facial authentication to verify the identity of the person taking the test. The following alerts ensure testing integrity and significantly reduce instances of identity circumvention. Alerts are generated when:
 - o The face does not match the enrolled participant
 - o Identity verification cannot be completed
 - o A different individual attempts to take the test
 - o Obstructions, lighting issues, or improper positioning impact verification
- + **Missed Test Alerts.** If the participant fails to complete a scheduled or on-demand test, the system generates a missed-test alert. Each missed test is accompanied by a GPS location captured at the scheduled testing time, allowing officers to compare reported whereabouts with verified device location.
- + **Low Battery and Critical Battery Alerts.** The device issues low-battery and critically low-battery alerts are automatically shown on each test.
- + **Courtesy Notification Alerts. Shadowtrack Application** can initiate text reminder to notify participants shortly before scheduled tests. This feature enhances client success rates and reduces missed tests. These reminders may include:
 - o Upcoming test alerts
 - o Value-Added Optional Check in Capability
 - o Value-Added Optional Location Based Monitoring of Locations
 - o Value-Added Optional Creation of Inclusion Zones and Exclusion Zones
 - o Value-Added Optional Face Time Video Conference
- + **Alert Management Through Monitoring System.** Supervising officers can manage all ShadowBriety alerts through the ShadowtrackONE monitoring platform, which allows them to:
 - o Review, resolve, and organize alerts by type, client, or caseload



- o Access detailed event data including photographs, GPS points, and testing sequences
- o Initiate on demand tests in response to alert activity
- o Initiate Value-Added Optional Check in Capability
- o Initiate Value-Added Optional Location Based Monitoring of Locations
- o Initiate Value-Added Optional Creation of Inclusion Zones and Exclusion Zones
- o Initiate Value-Added Optional Face Time Video Conference

Agencies configure alert rules for breath test violations, missed tests, identity mismatches, communication interruptions, and battery-related issues through the monitoring platform. Options include:

- + Assigning alert recipients by role or caseload
- + Choosing between real-time notifications or grouped alert summaries
- + Setting thresholds for when positive tests trigger mandatory confirmation testing
- + Configuring random, scheduled, and on demand testing windows and associated alerting

This flexibility enables agencies to align alert protocols with programming policy.

Alert Intervals and Communication Timing. Shadowtrack is designed for real-time reporting:

- + Each test's BAC, GPS point, and facial authentication result are transmitted immediately when cellular and/or Wi-Fi service is available
- + Device-initiated test windows ensure the unit powers on and prompts testing even without coverage
- + Missed test alerts include a GPS location captured at the scheduled test time

These communication safeguards ensure prompt reporting without loss of test data.

ShadowBriety includes security-grade features to ensure reliability:

- + Xtend® Fuel Cell Sensor, the same professional-grade technology trusted by hospitals, clinics, and law enforcement, and offers the highest level of accuracy and consistency.
- + Internal Breath Pump, mini solenoid breath pump ensures the most accurate and efficient breath capture for testing.
- + Bluetooth Connectivity wirelessly connects to the smartphone via Bluetooth. Compatible with most Apple and Google devices.
- + Advanced facial authentication prevents someone else from taking the test
- + High-resolution imaging and immediate on-screen user feedback reduce poor-quality or unverifiable photo captures
- + Use advanced facial detection technology to verify that a visible face is present. No face detected. Tester not facing forward. The test is automatically blocked.
- + Designed to prevent tampering, the test also stops if it detects more than one face.
- + Designed to keep every test honest, by requiring the Tester to show their face and preventing multiple faces on-screen.
- + Advanced feature that confirms the participant is blowing into the breath tub securely attached to the ShadowBriety - BACtrack device.



5. Describe your customizable reporting. How does the reporting work with court requests and chain of custody requirements for legal purposes.

SENTINEL RESPONSE

CUSTOMIZABLE REPORTING FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM Optix provides a comprehensive suite of customizable reports for SCRAM CAM and SCRAM Remote Breath Pro. Optix supports agency-specific, officer-specific, and client-specific reporting needs and allows users to configure reporting parameters to meet supervision requirements and court expectations. Key reporting capabilities include:

- + **Client Summary Reports** provide an overview of a client's performance for a selected date range. These reports can be generated by officer, agency, or court, and include alcohol test results, compliance history, and device-specific monitoring data for both technologies.
- + **Client Event and Program Reports** capture detailed monitoring events including alcohol readings, missed or taken breath tests, device prompts, tampers, and other key activities. These reports support both daily operations and evidentiary review.
- + **Administrative and Program Management Reports** include device-assignment history, installation and removal logs, billing summaries, and program-level activity reports to support internal auditing, reconciliation, and inventory management.
- + **Configurable Notifications and Reporting Parameters** where officers can define violation criteria, alert thresholds, and notification protocols at the client, officer, caseload, or agency level, ensuring reporting aligns with local supervision standards.

All reports are accessible from any web-enabled device at any time, ensuring continuous availability for program staff and judicial stakeholders.

COURT REQUEST SUPPORT FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM Systems maintains a comprehensive court-support program. Support features include:

- + **Court-Ready Documentation.** Reports are formatted for evidentiary submission and include complete event histories, alcohol-level interpretation, biometric verification (Remote Breath Pro), and any device-generated alerts.
- + **Dedicated Court Support Team.** SCRAM Systems provides event-specific testimony, evidentiary-hearing assistance, and expert interpretation of data.
- + **Officer and Judicial Training.** Training includes detailed instruction on interpreting CAM transdermal results—distinguishing environmental exposure from ingestion—and on reviewing Remote Breath Pro authentication photos, test results, and client-response patterns.

CHAIN OF CUSTODY FOR SCRAM CAM AND REMOTE BREATH PRO

SCRAM Systems preserves full chain-of-custody integrity through secure data handling, system controls, and documented quality-assurance measures. Key elements include:

- + **Secure, Centralized Data Storage.** All device data—including alcohol readings, breath test results, GPS points (Remote Breath Pro), tamper indicators, photos, and event timestamps—is stored in SCRAM Optix within a secure, audit-controlled environment.
- + **Permanent Event Logs.** Every monitoring event is captured with a permanent timestamp and cannot be altered, ensuring complete traceability from device generation through reporting.
- + **Quality Control and Assurance.** A formal national quality-control program ensures documentation accuracy and compliance with evidentiary standards across all service locations.



- + **Subpoena and Testimony Compliance.** When subpoenaed, SCRAM Systems assigns personnel directly responsible for the monitoring information to appear and testify, ensuring proper representation of chain-of-custody handling and data interpretation.

These processes ensure all data remains secure, verifiable, and legally defensible throughout its lifecycle.

CUSTOMIZABLE REPORTING FOR SHADOWTRACK SHADOWBRIETY (OPTIONAL)

The ShadowtrackONE platform is a powerful and complete community supervision tool, including a suite of comprehensive services implemented individually or as a complete solution, with no geographic restrictions. The platform is user-friendly and can operate as a standalone system or comfortably integrate with the agency's case management system. The ShadowtrackONE platform is accessible to authorized personnel needing participant access by computer and officer mobile app. Authorized personnel can manage caseloads from within the platform, using each tool or solution in the suite, or entering notes independent of any additional Shadowtrack activity.

Shadowtrack has a wide array of report options ranging from violation reports to inventory control that can be downloaded, printed, and/or exported in various formats. From within the monitoring platform, supervising personnel can easily review/download/print/export the activity of a single participant or generate additional reports specific to the Participating Entity's needs. Many of the reports already available were requested by other customers. Reports are available via various formats including PDF, Excel, etc.

- + Caseload at a Glance
- + Alcohol Monitoring Tests
- + Missed Test / Check in
- + Automated and Ad Hoc Reports
- + Event History
- + Multi-point client enrollment
- + Client deactivation
- + Analytics

CHAIN OF CUSTODY FOR SHADOWTRACK SHADOWBRIETY (OPTIONAL)

The Shadowtrack System is SOC II Certified and preserves full chain-of-custody integrity through secure data handling, system controls, and documented quality-assurance measures.

Key elements include:

- + **Secure, Centralized Data Storage.** All alcohol readings, breath test results, test location points, participant demographic details, and photos are stored in the Cloud within a secure, audit-controlled environment. Shadowtrack's activity is cloud-based, and access to the case management system or any of the raw data requires two-factor passcode identification and authorization along with other security measures.
- + **Permanent Event Logs.** Every monitoring event is captured with a permanent timestamp and cannot be altered, ensuring complete traceability from device generation through reporting
- + **Quality Control and Assurance.** A formal quality-control program ensures documentation accuracy and compliance with evidentiary standards across the country.
- + **Subpoena Compliance.** When subpoenaed, Shadowtrack immediately notifies Participating Entities and assigns personnel directly responsible for the monitoring information to provide requested information ensuring proper representation of chain-of-custody handling and data interpretation.

Shadowtrack ensures all data remains secure and legally defensible throughout the contract life cycle.



6. Describe your Customer Service, including at least the following:

- a.** Hours of operation.
- b.** Order procedures (how long to respond to order, delivery time frame). Delivery time after receipt of order? Describe online ordering procedures.
- c.** Product request response time (what is kept on hand at office vs ordering products) – inventory on hand.

SENTINEL RESPONSE

Sentinel owns, staffs, and operates both its Primary Monitoring Center and Secondary Monitoring Center. Sentinel owns both the primary National Monitoring Center located at Sentinel's Norco, California, corporate office) and a geographically redundant secondary back-up monitoring center in Atlanta, Georgia. Sentinel's monitoring centers are staffed with trained personnel 24/7/365 and at no time are monitoring services outsourced or subcontracted.

HOURS OF OPERATION

Our monitoring center is staffed 24 hours a day, seven (7) days a week with a supervisor always on duty and live operators cross-trained to support our suite of supervision services and products. This staffing allows Sentinel field staff and agency staff to call and speak with one of our monitoring experts at all times of the day or night. We currently employ more than 60 individuals to staff our continuous operations (24/7) facilities. This staff provides monitoring services at all times including real-time support to agency personnel for all the monitoring services we provide, including GPS tracking. Sentinel's comprehensive staffing enables agency personnel to call and speak with one of our monitoring experts at all times of the day or night. In addition, our monitoring center is staffed with bilingual personnel every shift to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants to triage certain alerts, regardless of the day of the week or time of the event.

Sentinel also provides access to designated help desk staff to assist with the needs/concerns of program agents including seven (7) specialized Help Desk staff. This specialized Help Desk support services department performs testing of critical or ongoing events and triages the events to the appropriate department(s) for permanent resolution. Sentinel is an innovator in providing this type of support and proactively 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 to the Regional Account Manager for customer enhancement requests, suggestions, and ideas.

—IMPORTANT SENTINEL ADVANTAGE—

Multiple Warehouse Distribution Centers

To aid our customers, Sentinel a Primary Warehouse located at 1220 North Simon Circle, Unit C, Anaheim, California as well as a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia. With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers. Both locations are open five (5) days a week during normal business hours from 08:00-17:00 daily.

ORDER PROCEDURES

Sentinel's Help Desk is the point of contact for the ordering of new equipment and the Return Material Authorization (RMA) process. New and return orders are received by the Help Desk via a SentinelDNA monitoring system submission, email, phone call or fax from the customer. Return Material Authorization (RMA) requests

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



submitted to Sentinel are received by the designated Help Desk representative who is responsible for ensuring the order is properly processed and the customer confirmation email is delivered.

In accordance with Sentinel's Ordering Process, all orders received by 12:30 p.m. (Local Time) are prioritized, processed, and shipped on the day the order is received. Orders received after 12:30 p.m. (Local Time) are processed and scheduled for shipment the next business day.

In accordance with Sentinel's shipping process, orders are prioritized and processed based on the expected Arrival Date at the customer's location. Sentinel staff add new orders received to the Open Orders Report. Once the order is ready to be processed, staff will print and review the Order Details Report for adequacy and prepare the order utilizing one of the shipping methods below. The staff will then change the order status to 'completed' and remove the order from the Open Orders Report once the order has been shipped.

Sentinel's standard shipping method is Ground shipping at no cost to the Participating Entity. For Entities that desire express shipping Sentinel also offers the following shipping methods.

+ Ground Shipping (1-5 business days)	+ 2 nd Day Early AM
+ Express Saver	+ Standard Overnight
+ 3 Day Shipping	+ Priority Overnight
+ 2 nd Day Air	

REQUEST RESPONSE TIME

Sentinel maintains a core inventory of high-demand electronic monitoring equipment at its U.S. distribution centers to support rapid order fulfillment. Requests for items maintained in inventory are typically processed and shipped within one (1) business day of request receipt. Inventory levels are actively managed based on historical usage and forecasted demand to ensure availability and consistent service levels. New devices are received weekly at our warehouse locations and at all times Sentinel maintains available inventory in both the Anaheim and Alpharetta warehouses to ensure timely delivery of customer orders. The volume of weekly deliveries may be increased or decreased based on forecasted needs to ensure warehouse inventory remains available at all times.

Additionally, Sentinel provides equipment for our customers that is stored at the customer's location. This "Shelf Stock" is available to address the day-to-day inventory needs of the program and to allow for ebbs and flows of program size without the need to order/return devices. The amount of Shelf Stock a customer chooses to utilize is determined by program operations, participant enrollments and duration of time on the program. Entities typically carry approximately 10%-15% of shelf stock at any given time.

7. How do you comply with local and state regulations (what type of research do you conduct when working with a new entity?)

SENTINEL RESPONSE

Sentinel strives to remain current and advocate support of legislative initiatives and regulatory initiatives in favor of, never in conflict with, Participating Entity initiatives. Sentinel has been providing electronic monitoring services since 1993 and today operates in more than 40+ states. Since inception, Sentinel has monitored social and political changes that have shaped the criminal justice system and the resulting alternative to incarceration programs where we provide services. Each state and local jurisdiction is subject to laws and regulations that Sentinel complies with both operationally and contractually. With the assistance of Sheppard Mullins, a leading law firm based in California, Sentinel reviews existing and pending legislation and accurately modifies contract documents, participating agreements, amendments, and adjusts operational procedures to remain compliant with local, state and federal regulations. When appropriate, Sentinel supplements our team with attorneys from local



jurisdictions to track and monitor legislation that is potentially impactful to the electronic monitoring industry and/or interests of our Entity partners.

When Sentinel receives an inquiry about our products and services or when we approach a government entity and they express a desire to learn about our continuum of products and services, our sales team will research the procurement requirements for that agency as well as research local and/or state statutes that stipulate the use of Cooperative Purchasing Programs. Sentinel has found this to be very effective in our consultative approach as once the agency determines they want to utilize Sentinel products and services, we share with them details on the researched statute and on the cost, time, and convenience, the NASPO ValuePoint Cooperative Purchasing Program and the Sentinel Electronic Monitoring Services Contract provides.

Sentinel understands and has experienced the regulatory nuances that must be addressed and complied with both contractually and operationally from county to county and state to state. Examples of Sentinel's regulatory understanding and compliance include the July 1, 2021, California Assembly Bill #1869 that removed various fees for the cost of administering home detention programs and continuous electronic monitoring. Sentinel tracked, communicated with our government customers, and modified all our impacted contracts to ensure continued compliance. Additionally, we modified our on-site equipment installation and collections services to comply with these new laws. Another example of staying abreast with regulatory requirements includes legislation in the state of South Carolina S.367/H3532 for bond release and requiring electronic monitoring providers to be approved by the South Carolina Law Enforcement Division (SLED). Sentinel has met the SLED Standards and is Certified in the State of South Carolina. Our local staff have completed the required background checks, drug testing and training in accordance with Sentinel and SLED standards. Our record keeping policies are performed in accordance with standards and the required SLED reporting is provided as required. As a SLED certified provider, Sentinel has facilitated information sharing by granting access to our monitoring system to law enforcement agencies.

All of Sentinel's products and services comply with applicable laws. All our products are FCC approved, registered, and certified as required by the cellular networks on which our devices communicate.

Sentinel does not distribute, sell, or otherwise share any information captured during the participant's electronic monitoring period and all records and data remain the sole property of the supervising entity. Moreover, Sentinel complies with all subpoena requests and has an internal Standard Operating Procedure that dictates the steps to be taken to secure evidentiary material and communicate with the legal stakeholders when a subpoena has been served.

Our attorneys along with our senior management team, which have more than 200 years of combined experience in the electronic monitoring industry, will continue to monitor legislative and regulatory changes to ensure ongoing compliance with all applicable laws. Further all future products are developed and certified by the FCC and cellular providers as required to comply with all local, state and federal regulations.

8. Describe the on-boarding process for new Participating Entity.

SENTINEL RESPONSE

SENTINEL ON-BOARDING PROCESS

Sentinel's customer on-boarding is a simplified and strategic process of guiding new Participating Entities through introduction of Sentinel field operations team and the initial planning session that includes discussions on agency setup, review of training curriculum, and discussions on the transition of the products and services to help them achieve their first "win" and value realization with the emphasis aiming to build confidence, improve efficiency, and establish long-term, productive relationships.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Following mutual authorization of the Participating Addendum, Sentinel works with the Participating Entity to finalize an On-Boarding Work Plan and Timeline that includes all known contacts, tasks, deliverables, milestones, and duration estimates for each task and resource loading for the duration of the project. We understand the importance of open and fully transparent operations in the provision of public safety solutions and believe it is essential to the effective operation of any electronic monitoring program. We meet with Participating Entity personnel weekly during the initial implementation stages to review progress, performance, and to identify and resolve any programmatic challenges.

After mobilization, Sentinel continues to meet with the Participating Entity as necessary monthly or quarterly depending on the needs of each Participating Entity. We continue to provide all written reports to the Participating Entity as needed to operate an efficient and effective program including participant activity reports for each program participant and monthly summary reports. In addition, the Sentinel Regional Account Manager continues to always be available through telephone and/or email communications to address concerns or resolve issues with the program.

We work closely with the Participating Entity to ensure all needs, including implementation timeline expectations, are met during implementation and transition. We are highly flexible in our capability for mobilization and adjust our plans and staffing requirements as needed per the decisions mutually agreed in the Initial Project Briefing and Information Session. The following is an example of the elements involved in Sentinel's On-Boarding Process:

On-Boarding Work Plan Milestone	Week 1	Week 2	Week 3	Week 4	Monthly Beginning at Program Start
Initial Project Briefing and Information Session: • Introduction of Sentinel Resource Contacts (Sales, Account Manager, Monitoring Center, Help Desk, Accounting/Billing) • Networking with other Sentinel Participating Entities for sharing Programmatic Policies and Best Practices • Confirmation/Schedule of Initial Order(s), Training and Transition • Agency Notification Profiling, what assistance, if any does the entity need with transferring existing program participants demographic data into Sentinel's Monitoring Application					
Pre-Production Project Evaluation and Analysis					
Design, Development and Testing					
On-site Program Staff Installation and Training					
Equipment Delivery					
Department Training					
Participant Enrollment & Equipment Transition					
Operation and Maintenance					
Assessment of Initial Order Fulfilment					
Ongoing Contract Monitoring and Reporting					



9. Describe the on-boarding process for new Clients. Include any installation information that may apply.

SENTINEL RESPONSE

PARTICIPANT ORIENTATION PROCEDURES

At the first meeting with staff, program clients are provided a full program Orientation. During this Orientation, the rules and regulations of the program are explained, and the client is required to sign the Participant Agreement, which has been customized to meet the needs of the program. Upon completion of the review of the Participant Agreement and based on the activities that the client is allowed to conduct, daily curfew schedules are established clearly detailing when the client can leave their residence for permitted activities.

Staff only allow those activities that are Participating Entity-approved and were established prior to program implementation. In order to verify their whereabouts while away from the residence, clients are instructed on what documentation is required for them to provide at all subsequent compliance appointments. The other tasks at the Orientation include:

- + **Schedule Review** | All daily curfew settings will be reviewed for accuracy and to verify compliance with Participating Entity-approved activities.
- + **Residential Confirmation** | The client will be required to provide proof of his/her residential location. Staff ask for proof of rent payment, monthly home payment note, or official correspondence that verifies the client's place of residence.
- + **Contact Verification** | The client will be asked to provide alternate contact methods. In addition to their personal telephone or cellular numbers, staff attempt to obtain other contact options including contact information for a spouse, friend, or other relative. These additional contact numbers are important when staff are researching an alarm or similar event. All these contact numbers are entered into the proprietary case management system.
- + **Fee Setting** | For those program clients requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule set up with the client.
- + **Next Appointment Setting** | Based on the required reporting schedule of the client, the next face-to-face meeting (Compliance Appointment) will be set at this time. The client will be provided with the appointment information as well as any required documentation that is needed to accompany them in order to ensure compliance.
- + **Question and Answer Support** | If there are any program related questions, the staff member will answer these for the client. If the client ever requests unusual changes such as a modification to their permitted activities, staff will immediately contact the designated Participating Entity personnel to inquire if the change(s) can be approved. Staff will NOT make any changes to the permitted activities or residential status without the prior approval of the designated Participating Entity personnel.

All this information is entered into the client's personal case file in the proprietary case management system, with copies of the statements also kept in the client's physical file at the program office. Participating Entity personnel can have secure access into the case management system to view all case manager-generated reports and notices at any time.

EQUIPMENT INSTALLATION PROCEDURES

Prior to the completion of the Enrollment process (further described below), staff install the required monitoring hardware on the client. As required, staff will perform all necessary steps for "installing" equipment, including enrollment within the SCRAM Optix monitoring system and/or ShadowtrackONE monitoring application, capturing initial enrollment images for visual compliance-related equipment, etc. The customary equipment installation procedures include:



- + **Preparation of Equipment** | Based on the level of monitoring required, staff will prepare the appropriate equipment type for installation. All equipment is tested by the Sentinel National Warehouse for performance prior to shipment to local field offices.
- + **Data Entry** | Staff will enter the required client information in the SCRAM Optix and/or ShadowtrackONE monitoring system as needed in order to activate the necessary alcohol monitoring or tracking equipment for said client.
- + **Sizing** | If ankle-worn equipment is required for the client, staff will size and fit the ankle-worn device on the client. This is accomplished by adjusting the hypoallergenic ankle strap down to an appropriate size and attaching it to the security holding buckle, which keeps the ankle strap in place.
- + **Installation** | The designated device is secured onto the assembled strap and buckle assembly.
- + **Activation** | The device is activated, and a "good hook-up" is confirmed in the SCRAM Optix and/or ShadowtrackONE monitoring system. This confirmation is done at the field office to ensure that the client's device is operating as required prior to their departure.
- + **Equipment Guide** | For situations where the client is issued multiple pieces of monitoring equipment, e.g. alcohol testing equipment, the staff member will instruct the client how to install the equipment at their residence, in addition to providing them with an instructional flyer illustrating the simple in-home install process if needed.

The Installation process is complete at this time and the monitoring and/or tracking equipment will begin to report all activity and alert information as required. The installation of an ankle device is completed in less than five minutes.

ENROLLMENT PROCEDURES

As the Orientation is being completed, staff create and submit an **Enrollment Notice** to the designated Participating Entity personnel thereby confirming the enrollment of the selected client has been completed. This enrollment notice contains all pertinent client and case information so that the Participating Entity knows all details of the supervision guidelines including the device type and serial numbers assigned to the client.

10. Provide screen shots showing the functionality and user experience of the web-based platform as well as the mobile platform.

SENTINEL RESPONSE

SCRAM CAM AND REMOTE BREATH PRO WEB-BASED PLATFORM AND MOBILE PLATFORM

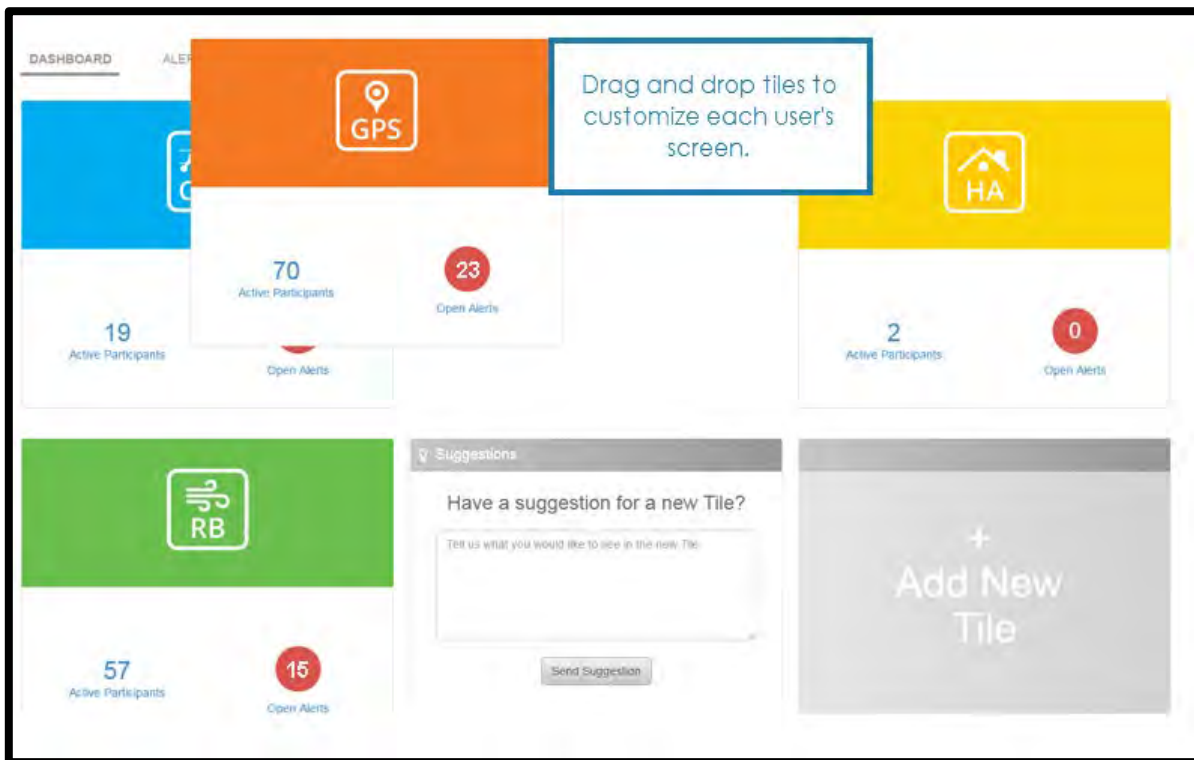
SCRAM Optix is a comprehensive, secure, and fully integrated supervision technology platform designed to support alcohol monitoring, location monitoring, and client engagement through both web-based applications and smartphone-based applications. These applications operate together to provide real-time data visibility, improve officer efficiency, and ensure the accuracy and timeliness of monitoring information. SCRAM Optix is secure, scalable, and accessible 24/7 via any web-enabled device. Officers can enroll clients, adjust device settings, enter/edit schedules, select notification methods or parameters, manage inventory and quickly access detailed caseload information at-a-glance via device and status indicators. It offers robust caseload and client management tools, including both point-by-point and advanced mapping with pattern of life features, inclusion/exclusion zone management, customizable notification protocols, and powerful program reporting tools.

Since mobile applications often have limited functionality, SCRAM Optix is designed to be mobile-adaptive, allowing users to access all features available on a computer or from a smartphone or tablet. Adaptive design can help ensure faster page load speeds and consistent user experience across different screen sizes. It requires no

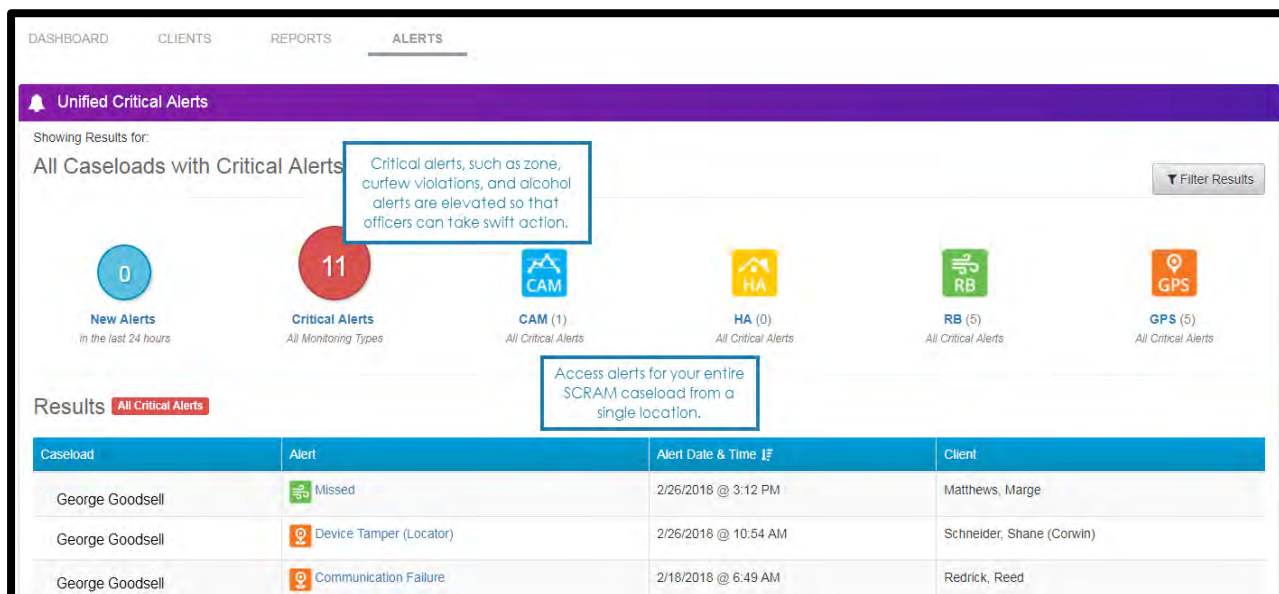
SCRAM Optix provides users with customizable views whereby the dashboard tiles can be arranged for easy access to the most frequently accessed devices, pages, and links.

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



SCRAM Optix provides Consolidated Alert Management whereby users can quickly see active clients by product type and view and access alerts for the officer's entire SCRAM caseload from a single location. Time sensitive alerts, such as tampers, alcohol use, zone, or curfew violations are elevated so that officers can take swift action.



The Client tab allows users to access a consolidated and searchable list of all clients they have permission to view across all SCRAM technologies: SCRAM CAM, House Arrest, and Remote Breath. Users are able to:

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + View a full list of clients in a single caseload or for an entire agency across all SCRAM monitoring types.
- + Search for active or inactive clients by first, last, or full name across all technologies.
- + Sort a client list by client name, caseload, or status (active or inactive).
- + Go directly from the client list to an individual client profile by clicking the View Profile link.

Dashboard
Clients
Reports
Alerts

Client List

Showing Results for:

All Caseloads

Search by Client Name

Status
Active

Monitoring Type

All
All
RB
CAM
GPS

Results

Client	Status	Caseload	Monitoring Type	Actions
Brummel, Bob	Active	George Goodsell		View Profile
Devries, Darrin	Active	George Goodsell		View Profile
Dungy, David	Active	George Goodsell		View Profile

SHADOWTRACK WEB-BASED PLATFORM AND MOBILE PLATFORM

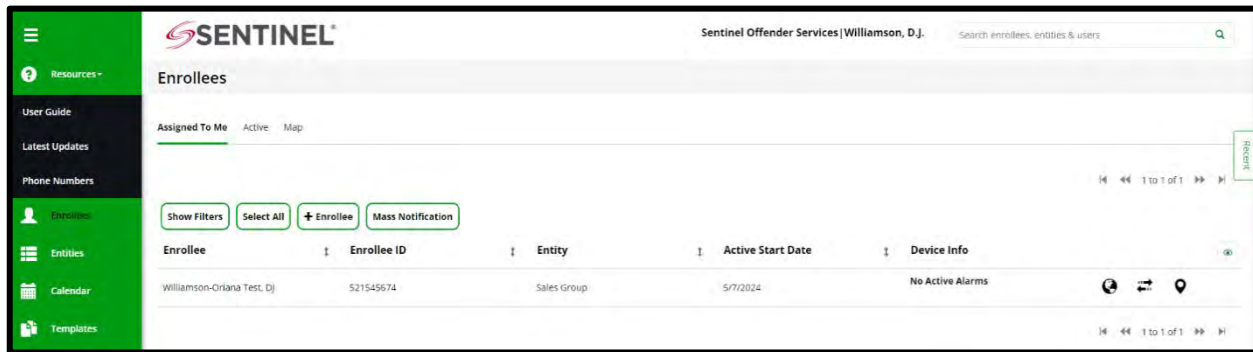
Shadowtrack is Intuitive designed to deliver real-time data tailored to the solutions being utilized, offering live insights to monitor performance, track engagement, and make informed decisions efficiently.



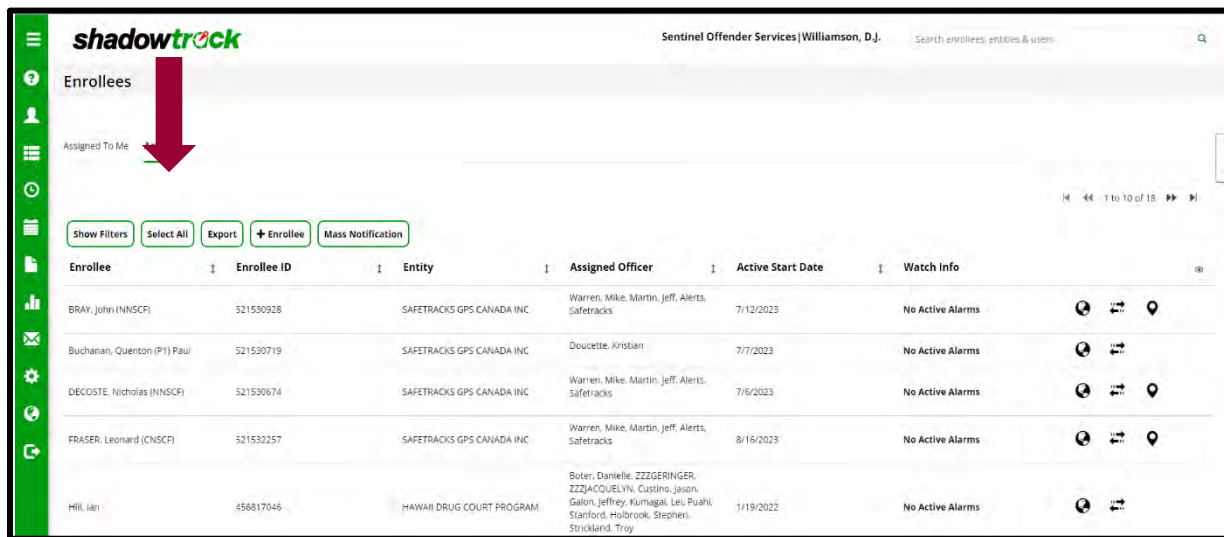
The Shadowtrack User's Guide is readily available for review from the left-hand menu under "Resources" and "User Guide." The "User Guide" is searchable to allow quick access to system information.

Request for Proposals for ELECTRONIC MONITORING

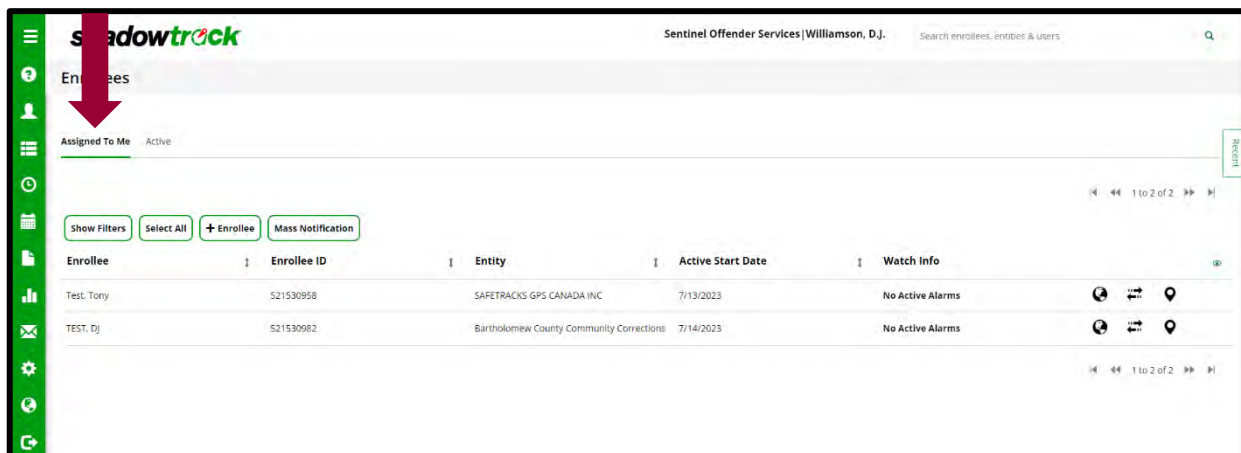
Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can easily navigate the Dashboard that displays all active participants within the agency.



Users can select from the Dashboard their Caseload that displays all active participants assigned to them.



Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can view Participant Location History and review zone locations within the software.

SENTINEL Sentinel Offender Services | Williamson, D.J. Search employees, entities & users

Williamson-Oriana Test, DJ Sales Group Add Internal Message Request

History Profile Zones Notifications Services Schedule Calendar Protocols Notes Documents Financial Check-ins

Locations Compliance Alarms

Show Filters Export 1 to 10 of 17

Date/Time	Status	Type	Compliance	Disposition	Location
Scheduled: 05/15/2024 11:30 AM EDT Completed: 05/15/2024 11:47 AM EDT	Complete	Interview Exceptions: 0 Questions: 4/4	Compliant	Complete Facial: Success	Inside Fence High Accuracy Location
Scheduled: 05/15/2024 10:33 AM EDT Completed: 05/15/2024 10:40 AM EDT	Complete	Video	Not Applicable	Complete	Location Verified High Accuracy Location
Scheduled: 05/15/2024 10:31 AM EDT Completed: 05/15/2024 10:32 AM EDT	Complete	Video	Not Applicable	Complete	Location Verified Medium Accuracy Location
Scheduled: 05/09/2024 01:25 PM EDT Completed: 05/09/2024 01:56 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	
Scheduled: 05/09/2024 01:00 PM EDT Completed: 05/09/2024 01:31 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	
Scheduled: 05/09/2024 12:32 PM EDT Completed: 05/09/2024 01:03 PM EDT	Complete	Curfew Outbound Facial Recognition	Non-Compliant Facial Recognition Expired	No Response	

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Zone Images including Satellite View and Alcohol Testing Results

Sobriety Results

	Image	Date	Sobriety Result	Facial Result
1		9/22/2025, 7:53 PM	Score 0.0000 Result Success	Score 100.00 Result Success

1 to 1 of 1

Call Location

Map
Satellite
Terrain



Call Location

Map
Satellite



Page **313** of **340**
Attachment 08, OFFEROR RESPONSE WORKSHEET

NASPO
ValuePoint

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can enter and edit Participants Profile Details

SENTINEL Sentinel Offender Services | Williamson, D.J. Search enrollees, entities & users

Williamson-Oriana Test, DJ 521345678 Sales Group Add Internal Message Request

Basic Information Details Edit

First Name: DJ Middle Name: Last Name: Williamson-Oriana Test Suffix: Internal ID: Primary ID: Image: [Profile Picture]

Email Address: Date of Birth: Language: English Time Zone: (GMT-05:00) East-Indiana/US Address: 71 Briarwood Court, Greentown, IN 46135, United States Assigned Users: Williamson, D.J., Hilbert, Thomas, Simmons, Eric, Brutto, Deana

Enrollment Phone Cases

Active: Yes Show History Update Active Dates

Active Start Date: 5/7/2024 10:49 AM Active End Date:

Enrollment Password: 16924784

Date of Voice Enrollment: [Field] Reses Enrollment

Date of Facial Enrollment: 5/7/2024 2:21 PM Enrollment Form

TFN Opt Out Date: [Field]

Users can create and edit Participants Zones (optional to program).

shadowtrack Sentinel Offender Services | Williamson, D.J. Search enrollees, entities & users

History Profile **Zones** Notifications Services Schedule Protocols Notes Documents Financial

Personal Shared

Map Satellite

Map View: A map showing a circular zone labeled 'HOME' in a residential area.

Zone Management:

- + Polygon + State/County + Circle
- 1 to 1 of 1

Name	Modified	Default	Exclusion
HOME	7/14/2023 10:54 AM by Williamson, D.J.	Yes	No

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can create schedules, edit Schedules, and View in a Calendar Based Format

The screenshot shows the ShadowTrack interface for Sentinel Offender Services | Williamson, D.J. The user is logged in as TEST, DJ (521530982). The interface displays a calendar for August 2023. A red arrow points to the 'Schedule' button in the top right corner of the calendar grid. The calendar shows a 'Meeting with C.' on August 11th. The right sidebar contains buttons for '+ Schedule', 'Enable', and 'Disable', and a table of scheduled events.

Type	Starts On	Recurrence	Status
Curfew Outbound Facial Recognition	07/14/2023 11:00 AM	Daily	Disabled Note:
Curfew Outbound Facial Recognition	08/04/2023 12:00 AM	Daily	Disabled Note:

Users can create Outbound Alcohol Test Schedules

The screenshot shows the SENTINEL interface for Sentinel Offender Services | Williamson, D.J. The user is logged in as TEST, DJ (521530982). The interface displays the 'Mobile Service' configuration page for an Outbound Alcohol Test Schedule. The configuration includes fields for Time Zone, Zone, Schedule Start Date, Period Start, Period End, First Window Start, First Window End, Enable Quiet Time, Send Silent Location Request, Quiet Period Start, Quiet Period End, Scheduling Type, Recurrence, Ends, This Date, Repeats Every, Minimum Calls Per Day, and Maximum Calls Per Day.

Mobile Service
Facial Recognition

Time Zone
(GMT-05:00) East-Indiana/US

Zone
Home

Schedule Start Date
05/09/2024

Period Start
9 : 00 AM

Period End
4 : 00 PM

First Window Start
05/09/2024 9:00 AM

First Window End
05/09/2024 4:00 PM

Enable Quiet Time
Send Silent Location Request

Quiet Period Start
HH : MM

Quiet Period End
HH : MM

Scheduling Type
Fixed Pattern

Recurrence
Daily

Ends
On

This Date
05/10/2024 5:00 PM

Repeats Every
1 Days

Minimum Calls Per Day
2

Maximum Calls Per Day
7

Request for Proposals for ELECTRONIC MONITORING

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Users can create Inbound Alcohol Test Schedules

shadowtrack Sentinel Offender Services | Williamson, D.J. Search enrollees, entities & users

Curfew Inbound Schedule: TEST, DJ

Enrollee Active Date is 7/14/2023, 10:39 AM

Select a template from the dropdown...

Preview Apply

Time Zone: (GMT-05:00) East-Indian/US

Schedule Start Date: 08/26/2023

First Window Start: 08/26/2023 7:00 AM

Zone: HOME

Period Start: 7 : 00 AM

First Window End: 08/26/2023 9:00 PM

0.03 mile radius

Radius Override (miles)

Period End: 9 : 00 PM

Allow Calls From Any Phone Number? Yes No

Inbounds Required: 4

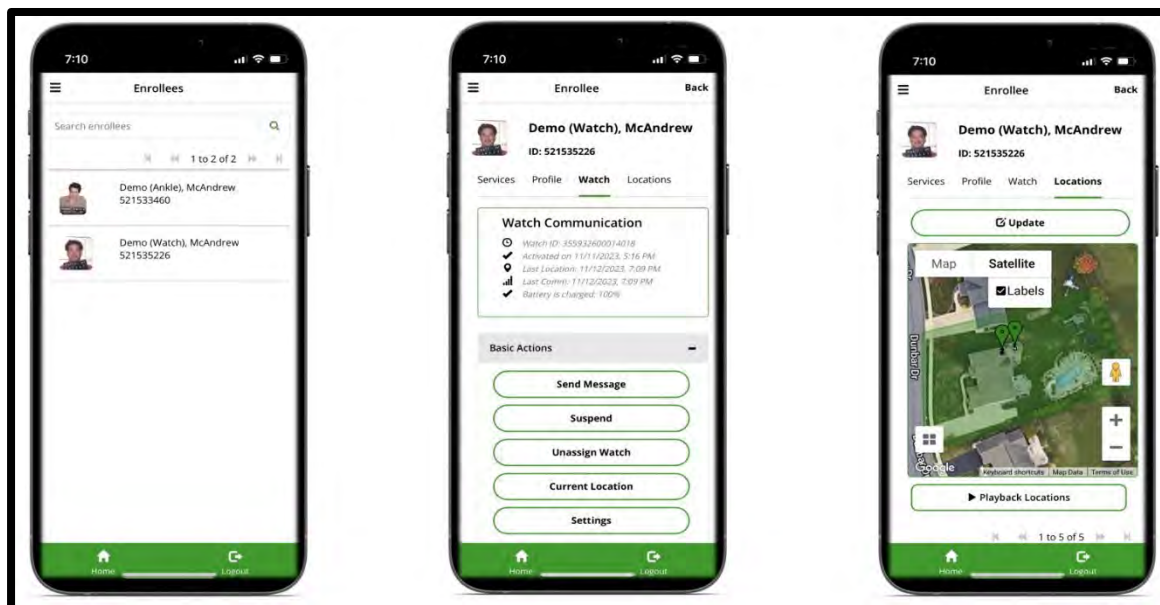
Recurrence: Daily

Ends: Never

Repeats Every: 1 Days

Save Schedule Cancel

Officer Mobile App allows officers to manage participant alcohol compliance from the palm of their hand.



11. Attach the Service Level Agreement for the Alcohol Monitoring product(s) you are proposing.

SENTINEL RESPONSE

SERVICE LEVEL AGREEMENTS

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements ("SLAs"). Please refer to the **Supporting Documentation** (page 340) of this document for Sentinel's Service Level Agreement for the Alcohol Monitoring products we are proposing.



D. CUSTOMER SATISFACTION

ALL QUESTIONS BELOW MUST BE ANSWERED REGARDLESS OF THE CATEGORY(IES) TO WHICH YOU ARE RESPONDING.

D. Customer Satisfaction.

1. Provide evidence of your customers' satisfaction with your product or services.

1. Client retention rate during the past 3 years
2. Customer surveys/references
3. Vendor performance ratings

SENTINEL RESPONSE

Today, more than 250 agencies throughout the United States are utilizing the Sentinel products and services. Sentinel's Director of Quality Assurance periodically distributes an NPS Survey to all customers to improve overall service quality. The survey includes evaluation of all aspects of our operation including the Monitoring Center and Help Desk services. The results of these surveys provide guidance for our continual improvement efforts and results are available to our customers at any time.

Our most recent customer survey was completed on December 18, 2025, where we continue to receive high marks from our customers, including those currently under the NASPO ValuePoint Master Agreement. The survey provided valuable insights into customer satisfaction, highlighting the strong value customers placed on Sentinel's Account Management and Help Desk support team. Respondents consistently noted the team's responsiveness, communication, quality of service, effectiveness in resolving and escalating issues, efforts to keep customers informed about new hardware, products, and services, and overall availability to support customers as needed. Customers expressed appreciation for having dedicated Account Managers who understand their business needs, communicate clearly, and act as trusted partners rather than transactional contacts. These findings reinforce the role of the Account Management team as a crucial driver of customer confidence, retention, and long-term relationship growth. The customer survey results demonstrate a high level of satisfaction with Sentinel's account management team and monitoring services support with an NPS score of 63, which indicates excellent results in the electronic monitoring industry, as shown in the following table.

Additionally, Sentinel utilized an outside firm (IGS) to survey customers on specific critical elements of our services, and we are pleased to report we received a score of greater than 98% on the following critical elements.

- + Range of Product Solutions
- + Reliability of Product Solutions
- + Price
- + Customizability
- + Customer Service
- + Device Accuracy
- + Geographic Coverage
- + Alert Escalation Times

For more than 30+ years Sentinel has maintained one of the highest customer retention rates in the industry. Our over 95% customer retention rate demonstrates that our customers are happy to provide Sentinel with a review



and testimonial on receiving reliable products and quality service at competitive rates allowing their officers to remain efficient and effective in the supervision of electronic monitoring participants.

Sentinel continues to outscore the competition in all the most critical areas identified by Participating Entities. Most recently, Sentinel was awarded one of the largest county contracts in the electronic monitoring market, Harris County, Texas, which monitors more than 2,000 active participants and requires value-added services, including a team of local staff supporting the day-to-day program operations. This RFP required review by Pretrial Services, Juvenile Probation, and CSCD. The results indicated that Sentinel outscored the next closest provider by approximately 6% and was the highest ranked vendor in each of the following categories including: IT Infrastructure and Cyber Security, Reliability and Accuracy of electronic monitoring equipment, Experience, Customer References, Success of providing monitoring services, Compliance with functional requirements technical requirements, and Compliance with state and federal laws. At Sentinel we are proud of our reputation in the electronic monitoring industry and believe our 30+ years and 95+% customer retention rate demonstrates our commitment to providing quality products and services to the agencies we serve.

—IMPORTANT SENTINEL ADVANTAGE—

Per the most recent NASPO ValuePoint Supplier Review, Sentinel remains the largest NASPO ValuePoint Contractor for Master Agreement #22PSX0021, confirming that both the EM industry and customer's continued preference is for Sentinel solutions.

2. Provide a brief history of your company.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

Sentinel Offender Services, LLC ("Sentinel") is one of the nation's leading providers of electronic monitoring/offender services and has twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement #22PSX0021. Sentinel has unparalleled experience in electronic monitoring and more specifically in successfully marketing national NASPO cooperative contracts, including but not limited to demonstrated by the following:

- + Sentinel's Management Team has over 200 years of combined experience directly within the Electronic Monitoring industry
- + For NASPO ValuePoint Master Agreement #22PSX0021, Sentinel is an incumbent Contractor in all three (3) categories, serving approximately fifty-four (54) Participating Entities
- + Since 2012, Sentinel has returned over \$440,000.00 in administrative fees to NASPO ValuePoint
- + Per the most recent NASPO ValuePoint Supplier Review, Sentinel remains the largest NASPO ValuePoint Contractor for Master Agreement #22PSX0021

Since our founding in 1993, Sentinel's core business operations have been solely focused on providing electronic monitoring services to criminal justice agencies nationwide. We are proud to remain an industry leader and to continue to bring innovative and progressive options to the agencies we serve. We provide 24 hours a day, 7 days a week, 365 days a year electronic monitoring and supervision services to 250+ agencies across the United States from our International Organization of Standardization (ISO) 9001:2015 Certified National Monitoring Centers and from highly trained staff nationwide. Our professional staff of nearly 290 employees is dedicated solely to providing services within the offender management market. Currently, we have operations in 40+ states, operate 20+ office locations across the country, and monitor tens of thousands of participants nationwide daily through our wide array of services, products, and programs. We have electronically monitored and tracked more than 2.5 million offenders and completed more than 10 million face-to-face meetings with program participants

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



ensuring compliance, addressing program fees, performing drug testing, changing participant schedules, and reporting to the agencies we serve. *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 32+ years of operation, we have provided a wide array of services to offender supervision programs nationwide. We monitor participants who are pre-trial, post-sentence, and in custody of those agencies we serve, *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 the agencies we serve. Corrections agencies, sheriff's departments, probation and parole departments, and courts can receive more electronic monitoring and offender management solutions through Sentinel than any other single service provider. These services include:

- + Global Positioning Satellite (GPS) Tracking
- + Radio Frequency (RF) Monitoring
- + Alcohol Monitoring and Testing Services (Breath and Transdermal options)
- + Victim Notification and Tracking Application
- + Case Management Services, including Court Testimony
- + Drug Testing Programs
- + Voice Verification Programs
- + Offender-Funded Programs
- + Smartphone Check-in / Video Call Applications
- + Wrist-Worn GPS Tracking Devices
- + Court Reporting Programs
- + Day Reporting Centers

Sentinel is the Original Equipment Manufacturer for our RF Patrol and our OM Series GPS solution. We have been providing offender monitoring services for 32+ years, Global Positioning Satellite System (GPS) equipment and tracking services for 28 years, and we have been providing Alcohol Monitoring Services for 31 years.

Sentinel has contracted with some of the most progressive and demanding correctional agencies in the provision of electronic monitoring, including for the services of radio frequency electronic monitoring, GPS tracking, and alcohol monitoring. Today, we serve correctional agencies at all levels of government. This entails state-level agencies that include the State of Alabama Bureau of Pardons & Paroles, the State of Connecticut Judicial Branch, the State of New Hampshire Department of Corrections, and the State of Hawaii Judiciary and Department of Public Safety. In addition, we are contracted with some of the largest county programs in the country including operations in Leon and Miami-Dade Counties within Florida; Bexar, Dallas, and Harris, Counties within Texas; Los Angeles, San Diego, and San Francisco Counties within California; Dauphin County and the City of Philadelphia within Pennsylvania; and in the Cities of Seattle and Tacoma, Washington, just to name a few. Sentinel also provides state-of-the art technology and services at the federal level including the District of Columbia Pretrial Services Agency and the District of Columbia Superior Court.

Sentinel's performance for these agencies, as well as to all our customers nationwide, demonstrates that we execute upon our commitment to providing services that meet or exceed the equipment and distinct service needs for each program. In addition, over the last 32+ years, we have gained unparalleled knowledge and experience in how to successfully design, implement, and operate programs that are based on clear communication and strict compliance with program requirements, and we are focused on providing the highest-level services to our customers.

Sentinel also has an extensive relationship with Alcohol Monitoring Systems Inc. (AMS) dba SCRAM Systems, the manufacturer of the proposed SCRAM Continuous Alcohol Monitoring (SCRAM CAM) bracelet that provides 24/7 transdermal alcohol testing for hardcore drunk drivers and/or repeat high-risk alcohol offenders as well as

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



the Remote Breath Pro handheld portable breath alcohol testing unit. As an AMS-authorized Service Provider, Sentinel is a direct extension of AMS and the hands-on representative in the field, offering comprehensive, responsive, and valuable services to Agencies. Sentinel's staff have undergone extensive training in every facet of SCRAM Systems operations and has undergone an extensive AMS certification process, so the result is best-in-class program development, excellent service execution, and technical innovation.

Our collaboration includes SCRAM Systems providing certified data analysts to review all CAM alcohol monitoring alerts with no need for the agency staff to initiate or request confirmation results, thereby, reducing officers/agency workloads. The collaboration between Sentinel and SCRAM Systems will provide Participating Agencies single-source admissibility.

Additionally, Sentinel is an authorized Value-Added provider of the Shadowtrack Technologies ShadoWatch, a wrist-worn GPS device, and Shadowtrack mobile applications. Sentinel has successfully deployed these services throughout the United States. ShadoWatch is a wrist-worn GPS device for monitoring and supervising low- to moderate-risk clients assigned to electronic monitoring or for those who are unable to wear an ankle device for medical reasons. Also used for low and moderate risk program clients, the Shadowtrack mobile applications utilize the client's mobile phone to allow the participant to check-in remotely as required by the agency, report on their schedules, provide confirmation of location, and directly communicate with agency officers. Our relationship with Shadowtrack provides for the utilization of ShadowBriety a comprehensive supervision tool designed for participants required to submit to alcohol testing featuring bluetooth and facial recognition technology.

It is important to note that Sentinel, as the prime contractor for any contracted services performed, maintains 100% responsibility. Sentinel **owns and operates** our National Monitoring Centers located in Norco, California, and Atlanta, Georgia. Our monitoring centers are staffed with Sentinel dedicated employees 24 hours a day, seven (7) days a week, 365 days a year with trained personnel and supervisors available on every shift. To additionally aid our eastern customers, Sentinel also has a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia 30005. **With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers.**

3. Describe your company's growth during the past three years.

SENTINEL RESPONSE

The number of participants and customer agencies serviced by Sentinel has increased significantly in the past three (3) years. While all vendors in electronic monitoring experienced a temporary increase in participant population during COVID, Sentinel has continued to expand the number of new customer agencies and participants monitored as the COVID impact has worn off. Our growth has accelerated through the acquisition of Omnilink Systems in 2022 and the robust sales success since that time. During this time, Sentinel has increased the number of participants actively monitored on any given day by more than 20% and now is one of the largest providers of electronic monitoring in the United States.

4. Describe your company's experience performing the same or similar Scope of Work or providing the same or similar Deliverables to other public sector customers.

SENTINEL RESPONSE

Sentinel has contracted with some of the most progressive and demanding correctional agencies in the provision of electronic monitoring, including for the services of radio frequency electronic monitoring, GPS tracking, and alcohol monitoring. Today, we serve correctional agencies at all levels of government. This entails state-level agencies that include the State of Alabama Bureau of Pardons & Paroles, the State of Connecticut Judicial

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



Branch, the State of New Hampshire Department of Corrections, and the State of Hawaii Judiciary and Department of Public Safety. In addition, we are contracted with some of the largest county programs in the country including operations in Leon and Miami-Dade Counties within Florida; Bexar, Dallas, Harris, and Tarrant Counties within Texas; Los Angeles, San Diego, and San Francisco Counties within California; Dauphin County and the City of Philadelphia within Pennsylvania; and in the Cities of Seattle and Tacoma, Washington, just to name a few.

Sentinel's performance for these agencies, as well as to all our customers nationwide, demonstrates that we execute upon our commitment to providing services that meet or exceed the equipment and distinct service needs for each program. In addition, over the last 32+ years, we have gained unparalleled knowledge and experience in how to successfully design, implement, and operate programs that are based on clear communication and strict compliance with program requirements, and we are focused on providing the highest-level services to our customers.

—IMPORTANT SENTINEL ADVANTAGE—

As one of the nation's leading providers of electronic monitoring/offender services, with twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement #22PSX0021, Sentinel has unparalleled experience in electronic monitoring and more specifically in successfully marketing national NASPO cooperative contracts, including but not limited to demonstration by the following:

- + Sentinel's Management Team has over 200 years of combined experience directly within the Electronic Monitoring industry
- + For NASPO ValuePoint Master Agreement #22PSX0021, Sentinel is an incumbent Contractor in all three (3) categories, serving approximately fifty-four (54) Participating Entities
- + Since 2012, Sentinel has returned over \$440,000.00 in administrative fees to NASPO ValuePoint
- + Per the most recent NASPO ValuePoint Supplier Review, Sentinel remains the largest NASPO ValuePoint Contractor for Master Agreement #22PSX0021

As a longer-term partner to NASPO, Sentinel has truly demonstrated and proven to serve as "*a one-stop shop*." We stand ready to continue providing services for the new Electronic Monitoring contract with technology and services to meet all categories required.

E. SOFTWARE INTEGRATION

- E.** Describe what, if any, software integration support that can be provided by the Contractor to integrate with a State's Offender Management System, if the State chooses to.

SENTINEL RESPONSE

Sentinel has developed and does support Application Programming Interfaces (APIs) to interface our electronic monitoring system with external systems. The Sentinel Software Development Team has extensive experience in developing and testing APIs, using best in class software development practices and tools such as Postman and REST Assured, and JMeter performance/load testing, to develop and test secure, robust and scalable API interfaces. Key technologies used include REST, JSON, JWT, and Webhooks.

Implementing an API would require an engagement between Sentinel and the contracting State's technical team(s) to understand the exact requirements, project scope, and infrastructure needs to implement the APIs and requested integration with a State's Offender Management System. Upon completion and agreement on the Project Scope Document, Sentinel would deliver the necessary API and/or integration for the contracting State and support our portion of this project to ensure system performance and uninterrupted data exchange.



F. ARTIFICIAL INTELLIGENCE

- F.** Describe what, if any, artificial intelligence technologies you will be using in your performance of a Master Agreement resulting from this RFP and how and for what purposes such technologies would be used. Include any future plans for use of AI for products and/or services.

SENTINEL RESPONSE

Sentinel has been establishing data management systems within our Oracle Gov Cloud environment to scale AI-driven intelligence, ensuring that our analytics are powered by the most secure and comprehensive datasets available. Specifically, our process will focus on officer efficiency capabilities, device performance metrics, monitoring center engagement and processes designed to improve program outcomes.

Examples of Sentinel's use of AI-driven intelligence include utilizing our Analytics to evaluate zone sizes, curfews/schedules and travel distances to better align those three (3) elements to reduce the number of violations and thereby improve officer efficiency. We will further build out our Point Pattern Analysis (PPA) offering with AI allowing us to drill further into travel patterns, speed, location and compliance, such as zone, curfew, or tamper, to provide officers with advanced notice of future non-compliance. We will also use AI to measure and monitor internal device performance and perform diagnostics that will reduce device failures and increase the performance life of the device, thus reducing the number of service calls required by our agency partners/or Sentinel staff.

Collectively, in coordination with our agency customers, Sentinel will use AI to evaluate all programmatic inputs (case type, charge/offense, participant demographics, substance abuse testing, employment, etc.) to model and predict program outcomes and more importantly, appropriate participant engagement that promotes participant compliance and reduces recidivism.

The ideas presented here are a starting point that will be more fully developed with direct input from our agency customers. By placing the data in a usable format we are positioning ourselves for the best AI experience possible.

G. SUPPLY CHAIN

- G.** Describe the supply chain for electronic monitoring equipment. How long is the lead time to acquire equipment? Where is it shipped from. Are the products made outside of the USA?

SENTINEL RESPONSE

Sentinel's supply chain is resilient and reliable, supported by long-term supplier relationships and proactive demand planning. Supply chain status is reviewed weekly by Operations leadership in coordination with Purchasing and Engineering teams. No interruptions have been observed. Forecasts are provided to suppliers to meet expected demand at the right time, place, and quantity. Unlike other vendors, Sentinel has been able to maintain a steady supply chain during and since COVID and has been able to meet the demands of our customers when others have not.

Our Senior Vice President of Operations reviews supply chain status on a weekly basis with our Purchasing Department and Engineering teams. Sentinel utilizes an 18 - 24 month rolling forecast to purchase items with long lead times and mitigate supply risk. Sentinel receives new devices every week in accordance with our forecast. We can increase the number of GPS devices received weekly by simply updating our product manufacturer that is in Alberta, Canada. Devices are shipped to our warehouses in Alpharetta, Georgia, and Anaheim, California, for



final assembly, testing, packaging and consumable attachment. Sentinel's RF Patrol equipment is assembled in house from our location in Anaheim, California.

Standard electronic monitoring equipment maintained in inventory is available for shipment within one (1) business day.

Components used in manufacturing are sourced by our equipment manufacturer with parts and components procured in advance for 18 – 24 months of supply. Finished electronic monitoring equipment is manufactured at multiple North American facilities in Canada and Arizona and transferred to Sentinel's U.S. distribution centers in Anaheim, California, and Alpharetta, Georgia, for customer fulfillment, enabling timely domestic delivery and continuity of service.

All third-party equipment proposed are shipped from within the United States and received at Sentinel warehouse facilities.

- + SCRAM products are shipped from Littleton, Colorado, where they are manufactured and assembled for shipment within 48 hours of order receipt
- + Shadowtrack products are shipped from Covington, Louisiana where devices are manufactured and assembled for shipment within 48 hours of order receipt.

H. QUALITY ASSURANCE AND HARDWARE RETURNS

H. Quality Assurance and Hardware Returns.

1. What are your quality assurance measures and how are they handled in your organization?

SENTINEL RESPONSE

Sentinel uses Key Performance Indicators (KPI) to measure our performance by tracking specific, measurable metrics like product defect rates and compliance with contractual obligations. Sentinel has both global KPIs as well as those established at the branch level. KPIs are crucial for measuring the effectiveness of services by providing data-driven insights into performance, customer satisfaction, and operational efficiency. They transform complex data into clear, quantifiable information that helps organizations align efforts, make informed decisions, and achieve strategic goals.

Since September 19, 2010, Sentinel has been dedicated to delivering quality services, equipment, and a web-based information system and has achieved and maintained International Organization of Standardization (ISO) 9001 quality certification for Design, Production, and Delivery of Electronic Monitoring Technologies, Monitoring Center Services, Case Management Services, and Community-Based Offender Management Programs. Our leadership is committed to planning and defining KPIs at multiple levels throughout the organization and has established quality objectives at relevant functions, levels, and processes for our Quality Management Program that are monitored, communicated, and updated monthly to document our quality objectives and the results.

Quality objectives are reviewed to ensure continuing suitability, adequacy, effectiveness, and alignment with Sentinel's strategic direction. Sentinel management performs an analysis of the data from KPIs for conformity of our products and the conformity of our services as well as the performance and effectiveness of both. Sentinel deals with all aspects of participants, from monitoring center out-bound calling, command center inbound communications, face-to-face interviews, supervision, and case management services, including daily fee collections. We draw upon all our experience to provide world-class programs to successfully achieve the goals and objectives of our customers, the prevention and reduction of criminal activity, and the prevention of delinquency through Best Practices and improved community supervision practices and procedures.



We consistently demonstrate to our customers that we are a good partner by assisting them in achieving their goals. Sentinel works with our customers to continually recognize the changing needs of the offender supervision industry to ensure that we consistently deliver high quality service. Also, we recognize that our ability to provide the required and necessary equipment and services is facilitated by the professional relationship and cooperation established and maintained between our company and the staff of the agencies we serve. Our commitment is to assign well-qualified and trained staff who are aware of the critical functions for each of our programs. Our staff is dedicated to ensuring open lines of communication to facilitate change when necessary and offer suggestions when appropriate to promulgate better program results.

—IMPORTANT SENTINEL ADVANTAGE—

Sentinel is dedicated to delivering quality services, equipment, and a web-based information system and has achieved and recently successfully completed a recertification audit that confirms our quality management system meets the requirements of the ISO 9001:2015 standard. **Sentinel's ISO certification encompasses Design, Production, and Delivery of Electronic Monitoring Technologies, Monitoring Center Services, Case Management Services and Community-Based Offender Management Programs.** All of Sentinel's facilities and case management field offices are also certified under the ISO certification. ISO Certification is important to our customers as it demonstrates 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.

2. Describe your return policy for hardware.

SENTINEL RESPONSE

All requests for hardware returns are handled by Sentinel's Help Desk department. Requests are faxed, emailed, or called in by the Participating Entity and processed within one (1) business day of request. Each returned product is inspected to determine if there is a non-conformity or not. If a non-conformity is found, the product is returned to the manufacturing department and/or vendor for repair. If the product is found to be conforming upon initial testing, it will be fully tested to ensure that it meets all of the required specifications and re-circulated into the system for return to the field.

All returned equipment is also tracked for trending purposes with as much information as possible and returns are analyzed to determine where product and inspection improvements can be made. Key Performance Indicators (KPIs) have been created and are reviewed against returned equipment to ensure equipment is performing as required.

Sentinel handles customer returns through our Return Material Authorization (RMA) policy. Sentinel's RMA policy authorizes customers to return product and the disposition of the product to Sentinel. All requests for product returns are handled by Sentinel's Help Desk department. Requests are faxed, emailed, or called in by the Participating Entity and processed within one (1) business day of request. Additionally, Sentinel allows its customers to request formal evaluation reports for equipment being returned to control non-conforming product and evaluate the need to prevent recurrence.

All products returned on an RMA are received at our National Warehouse and inspected for quality in accordance with Sentinel's Receiving and Shipping process. Each returned product is inspected to determine if there is a non-conformity or not. If a non-conformity is found, the product is returned to the manufacturing department and/or vendor for repair. If the product is found to be conforming upon initial testing, it will be fully tested to ensure that it meets all the required specifications and re-circulated into the system for return to the field.

All returned equipment is also tracked for trending purposes with as much information as possible and returns are analyzed to determine where product and inspection improvements can be made. Key Performance Indicators



(KPIs) have been created and are reviewed against returned equipment to ensure equipment is performing as required.

I. IMPLEMENTATION AND PROMOTION OF NASPO

I. Implementation and Promotion of the NASPO ValuePoint Master Agreement.

1. Describe your company's experience working with contracting cooperatives.

SENTINEL RESPONSE

As one of the nation's leading providers of electronic monitoring/offender services, with more than twenty-five (25) years of direct experience as an incumbent Electronic Monitoring contractor for WSCA Master Agreement #14600, NASPO Master Agreement #00212, and NASPO ValuePoint Master Agreement # 22PSX0021, Sentinel has unparalleled experience in the provision of electronic monitoring services, providing participating entities enhanced value-added equipment and services, and more specifically in successfully marketing national cooperative contracts such as NASPO ValuePoint. As a long-term partner to NASPO, Sentinel has truly demonstrated and proven to serve as "a one-stop shop."

For over 25 years, Sentinel has championed its partnership with NASPO, delivering significant value to agencies nationwide, while offering the convenience and benefits offered through NASPO ValuePoint. The NASPO ValuePoint Master Agreement remains Sentinel's primary cooperative vehicle, allowing us to leverage our status as a leading provider across all NASPO categories. By integrating our robust service offerings, comprehensive field applications, and world class customer support services, we have successfully expanded the NASPO footprint into some of the nation's largest jurisdictions. Today, Sentinel is proud to be the most active user of the NASPO Master Agreement within the electronic monitoring industry, and we stand ready to continue providing services for the new Electronic Monitoring contract with technology and services to meet all categories required.

2. List the cooperatives through which you currently have a contract, and provide sales volume information for each. Identify any restrictions on pricing and sales (e.g., most-favored nation clauses) imposed by your other cooperative contracts.

SENTINEL RESPONSE

For more than 25 years Sentinel has promoted the use of NASPO ValuePoint as our primary cooperative purchasing agreement. Under the new agreement Sentinel will continue to utilize NASPO as our desired partner for all state and local government entities that have procurement statutes that permit the use of the NASPO ValuePoint cooperative agreements. The following is a list of current cooperative contracts Sentinel holds including the associated sales volumes which demonstrate clearly Sentinel's preference to utilize NASPO ValuePoint's Master Agreement whenever possible. Under the new NASPO Master Agreement Sentinel will continue to prioritize and promote NASPO ValuePoint as our preferred cooperative purchasing vehicle for every opportunity that allows its use.

+ **NASPO** (National Association of State Procurement Officials) ValuePoint

The total sales under our NASPO ValuePoint Contract for 2025 were \$14,714,015.93.



+ **GSA Advantage** (General Services Administration)

GSA Advantage is the federal government's online shopping superstore giving access to millions of commercial products and services available through pre-negotiated Schedule contracts utilizing the Cooperative Purchasing and Disaster Purchasing Programs. While primarily used by Federal Government Entities, State and local governments can take advantage where permitted by their state or local procurement statutes and access Most Favorable Customer Pricing based on the identified Scope of Work.

The total sales under our GSA Advantage Contract for 2025 were \$1,615,430.00.

+ Pennsylvania Office of General Services **COSTARS** Program

COSTARS is the Commonwealth of Pennsylvania's cooperative purchasing program and serves as a conduit through which registered and eligible Pennsylvania local public procurement units and Pennsylvania state-affiliated entities can leverage contracts established by Department of General Services to procure equipment and services for potential cost savings and their convenience.

The COSTAR Cooperative Purchasing Agreement is exclusive to Pennsylvania government entities that are registered with the DGS and officially members of the COSTAR Program.

The total sales under the COSTARS Cooperative Program for fiscal year 2025 were \$665,008.00.

+ North Carolina Sheriff's Association (**NCSA**)

North Carolina Sheriffs' Association maintains a Cooperative Purchasing Program that offers access to Technology and is open to all North Carolina county and city government entities for their convenience. Sentinel's cooperative purchasing agreement offers a 10% discount on our electronic monitoring equipment and services.

The total sales under the NCSA Cooperative Program for fiscal year 2025 was \$71,921.00.

+ Virginia Sheriff's Association (**VSA**)

Virginia Sheriffs' Association maintains a Cooperative Purchasing Program that offers access to Technology and is open to all Virginia county and city government entities for their convenience. Sentinel's cooperative purchasing agreement offers a 10% discount on our electronic monitoring equipment and services.

The total sales under the VSA Cooperative Program for fiscal year 2025 were \$0.00.

Sentinel's single largest cooperative contract is by far NASPO (the others collectively are a fraction of NASPO).

—IMPORTANT SENTINEL ADVANTAGE—

Per the most recent NASPO ValuePoint Supplier Review, Sentinel remains the largest NASPO ValuePoint Contractor for Master Agreement #22PSX0021. Since 2012, Sentinel has returned over \$440,000.00 in administrative fees to NASPO ValuePoint.

There are no known restrictions on pricing and sales imposed by Sentinel's other cooperative contracts.



3. Describe how you intend to market your Master Agreement and encourage participation among potential Participating Entities, including state governments.

SENTINEL RESPONSE

Sentinel will continue to leverage its position as the leading user of the NASPO ValuePoint Master Agreement to further expand participation. Our strategy focuses on visibility, education, and seamless onboarding to ensure state governments and eligible entities know about the continuum of products and services available via NASPO ValuePoint through rigorous sales and marketing campaigns, and the ease of use for their cost savings and convenience.

1. DEDICATED DIGITAL PRESENCE

We will maintain a landing page on the Sentinel corporate website specifically for the NASPO ValuePoint contract. This portal will feature:

- + **Authorized Branding:** Proper use of NASPO ValuePoint logos to signal credibility and compliance.
- + **Direct Connectivity:** Active backlinking to the Master Agreement for real-time access to terms, pricing, and documentation.
- + **Resource Center:** Downloadable guides that simplify the procurement process for state and local purchasing authorities.

2. INDUSTRY ENGAGEMENT AND TRADE EVENTS

Sentinel proactively promotes the NASPO ValuePoint cooperative purchasing agreement at major government technology conferences and procurement trade shows. Our displays, and collateral will prominently feature NASPO-approved graphics. Our goal is to ensure that when entities think of streamlined procurement, they associate it with the Sentinel-NASPO partnership.

3. DATA-DRIVEN CUSTOMIZED CAMPAIGNS

Utilizing our Salesforce CRM, Sentinel's Marketing and Inside Sales teams will execute targeted outreach campaigns utilizing email, LinkedIn, and social media efforts designed to:

- + Identify and reach out to state and local agencies that have not yet executed a Participating Addendum.
- + Track engagement and monitor interest levels to provide rapid follow-up with the specific technical data or "how-to-buy" instructions required to move forward.
- + Deliver tailored content that highlights the cost-savings, benefits, and administrative efficiencies inherent in the NASPO ValuePoint Master Agreement.

4. DIRECT SALES INTEGRATION

The NASPO ValuePoint agreement is not just a "tag-on" to our sales process—it is a core component. Our entire Sales Team and Account Management team are trained to:

- + Advocate for NASPO ValuePoint and educate potential customers on the pre-vetted nature of the contract, which reduces the need for lengthy individual RFPs.
- + Guide potential entities through the exact steps required to join, from initial interest to the signing of a Participating Addendum.



- + Include a dedicated NASPO ValuePoint mention in agency-facing presentations to ensure the Master Agreement is always front-of-mind.

Sentinel markets the Sentinel/NASPO Master Agreement via all leading methods:

- + Sentinel's entire Sales Team is fully experienced at promoting the Sentinel/NASPO Master Agreement and negotiating Participating Addendums
- + Sentinel's main corporate website is already configured to include a page dedicated to NASPO
- + Sentinel exhibits at multiple National Trade Shows as well as Regional Trade Shows

Sentinel markets the Sentinel/NASPO Master Agreement to all three EM market segments:

- + Incumbent Sentinel Customers in lieu of re-RFP
- + Competitor Customers
- + New Program Prospects

Sentinel markets the Sentinel/NASPO Master Agreement to contacts at all three levels of government:

- + Senior Administrative
- + User/Officer
- + Procurement

4. Describe features of the dedicated website you will be setting up for this Master Agreement, including, as applicable, customized price lists for each Participating Entity, staff contact information, and online ordering capabilities.

SENTINEL RESPONSE

DEDICATED WEBSITE

Sentinel will launch a comprehensive, user-centric website designed in collaboration with NASPO ValuePoint to serve as a primary resource for all Participating Entities. This site will act as a "single source of truth" for the Master Agreement, ensuring that procurement is efficient, transparent, and fully compliant. Key features and functionality of the website include:

- + **Streamlined Online Ordering:** The site will feature an online quote request and ordering engine. This system will allow authorized users to select products or services, generate quotes for internal approval, and submit purchase orders directly through a secure interface.
- + **Interactive Onboarding & Educational Hub:** To encourage participation, we will host a "How-to-Buy" resource center. This includes step-by-step guides, video walkthroughs on the PA process, and links to the NASPO ValuePoint Master Agreement for immediate reference.
- + **Direct Access to Subject Matter Experts (SMEs):** The portal will feature a dedicated contact directory, providing direct phone and email access to the Sentinel NASPO Account Team, including contract administrators and technical support staff assigned to specific regions.
- + **Analytics:** The site will track engagement and traffic. This allows our marketing and sales teams to identify which agencies are researching the contract and proactively reach out to assist them with the participation process. If a potential entity spends time reviewing specific price lists or educational content, our team receives an automated alert. This allows Sentinel to provide proactive, white-glove assistance to help that entity finalize their participation steps.



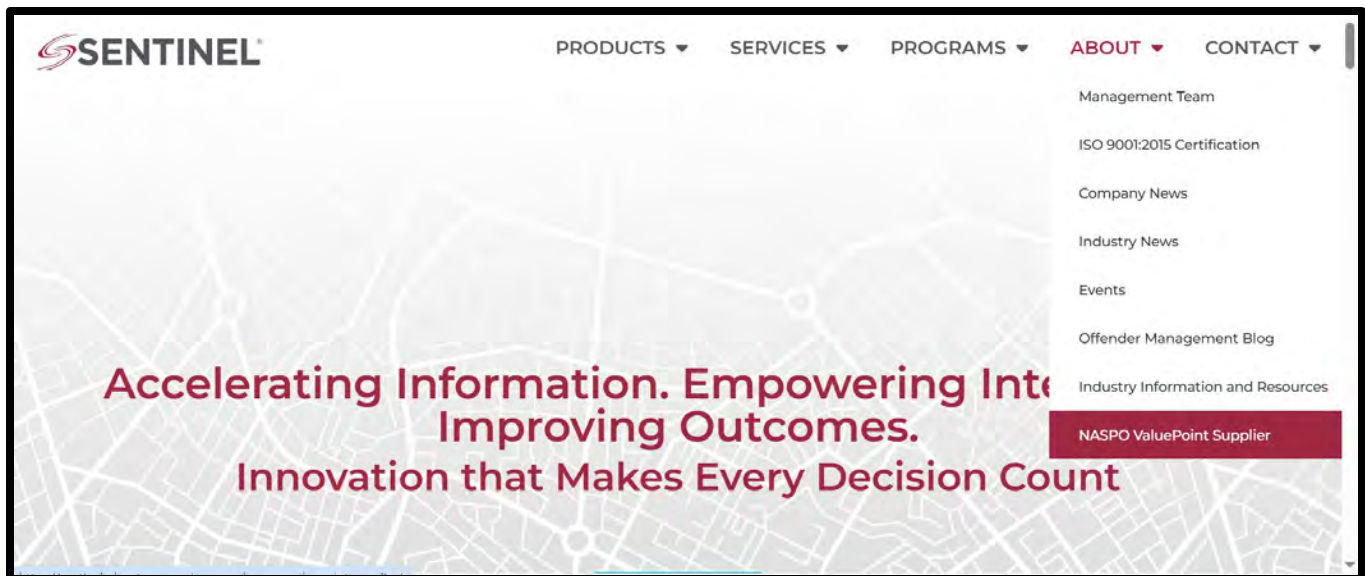
MAINTENANCE AND COMPLIANCE

Sentinel's marketing and web development teams will work in lockstep with NASPO ValuePoint to ensure all branding and content meet strict approval standards. We commit to:

- + **Continual Updates:** Sentinel will work closely with NASPO Valuepoint to ensure the website is continually updated with any changes related to the Master Agreement or NASPO policies.
- + **Collaborative Oversight:** All content, branding, and NASPO ValuePoint logos will be vetted by NASPO leadership to ensure 100% brand consistency.
- + **Continuous Evolution:** Our Marketing and IT teams will perform quarterly reviews of the site's performance, updating technical specifications and price lists to reflect the most current offerings.
- + **Document Vault:** A centralized place where entities can download the original RFP, the Master Agreement, and COIs (Certificates of Insurance) without having to email a Sentinel representative.

Sentinel's main corporate website is already configured to include a page dedicated to NASPO (<https://sentineladvantage.com/approved-naspo-valuepoint-supplier/>), that includes:

- + Description of Sentinel/NASPO and benefits
- + Contractor contacts for NASPO
- + Links to view/download:
 - o Master Agreement/Pricing
 - o Sample Participating Addendum
 - o Sentinel's NASPO RFP Response





5. Describe the staff and other resources that will be allocated to your Master Agreement and the training you will provide to staff to ensure their familiarity with Master Agreement terms and pricing and their compliance therewith.

SENTINEL RESPONSE

—IMPORTANT SENTINEL ADVANTAGE—

As a leading provider of electronic monitoring services and as a NASPO ValuePoint contractor for more than 25 years, Sentinel has established processes and protocols to effectively deliver services via NASPO ValuePoint agreements. Sentinel will continue to ensure familiarity with the Master Agreement including all terms and pricing.

The NASPO ValuePoint Agreement will receive full attention of Sentinel's Senior Leadership team as evidenced by the fact Sentinel is appointing Mr. Mike Dean, Sentinel's Senior Vice President of Sales as the point of contact for the NASPO ValuePoint Master Agreement.

MIKE DEAN | Senior Vice President of Sales

- + Mr. Dean oversees all Sentinel sales personnel and manages the company's cooperative purchasing agreements. With over 33 years in the electronic monitoring industry overseeing sales and contracting for some of the largest electronic monitoring providers, including BI Incorporated, 11 years, G4S Justice Services, 7 years, and Sentinel for the past 14 years, Mr. Dean has unparalleled expertise in collaborating with Federal, State, and Local Governments, developing electronic monitoring programs and leveraging cooperative purchasing to the benefit and convenience of government agencies.
- + Mr. Dean has worked directly with procurement departments negotiating Participating Addendums and reviewing contractual requirements for entities that makes him an exceptional subject matter expert and primary point of contact for the NASPO ValuePoint Cooperative Purchasing Agreement. Mr. Dean holds a Bachelor Agreement in Criminal Justice, from the University of Cincinnati, and as Senior Vice President of Sales, Mr. Dean is strategically positioned to champion the NASPO ValuePoint agreement. He will provide oversight for the NASPO ValuePoint Master Agreement and for the agency's participating addendums, programs and purchasing department, while also facilitating all post-award implementation adjustments required for this contract.

Mr. Dean will work closely with the Sentinel Field Operations Team and have complete support from our Chief Operating Officer, Mr. Darryl Martin. Mr. Martin has been overseeing the delivery of electronic monitoring services to the NASPO ValuePoint Agreements for more than 25 years. Mr. Martin will exercise all Sentinel departments and employee base of more than 280 to ensure complete compliance with the Master Agreement including the following resources that stand ready to continue providing services.

OPERATIONAL RESOURCES

With more than 280 employees across the country, Sentinel's extensive depth of field services personnel will provide corporate oversight for the contractual cycle of each of the Participating Entities during the program lifecycle. Field services personnel will be responsible for scheduling training, per the contract, with agency staff on the use of equipment, software and report interpretation. This strong nationwide presence of qualified Sentinel staff will ensure that the Participating Entities' needs are met satisfactorily and expediently, guaranteeing the highest possible quality of service for the Participating Entities. Our field services staff and monitoring center operations will continue to be led and receive the support of:

DARRYL MARTIN | Chief Operating Officer

Mr. Martin possesses over 30 years of direct experience in the electronic monitoring industry. His prior experience includes eight (8) years at Digital Products Corporation followed by nine (9) years at Sentinel Offender Services, where he served as Vice President and General Manager. In 2007, he transitioned his career to G4S Justice Services and held executive level responsibility for that company's nationwide monitoring centers, customer and



technical support, and internal operations before becoming its president. In 2012, Mr. Martin assumed the role of Chief Operating Officer of Sentinel Offender Services, LLC, through Sentinel's acquisition of G4S Justice Services. As Chief Operating Officer, Mr. Martin maintains executive responsibility for Sentinel's internal, logistical, and field operations, which include the company's network of field offices that specialize in community-based case management programs designed to aid program participants. Mr. Martin received his bachelor's degree in organizational leadership from Chapman University and received his MBA in Business Administration from the University of Redlands.

MELISSA STARR | Senior Vice President of Field Operations

Mrs. Starr is responsible for the management and oversight of our Regional Account Management team as well as Sentinel's national network of customer support and branch office personnel. This team manages the day-to-day needs of our benchmark offender-funded programs as well as providing customer service to our agency-funded contracts across the United States.

With a focus on the development of Standard Operating Procedures (SOP), attention to Key Performance Indicators (KPI) and relationship building, the Field Operations Team strives to make use of Sentinel's spectrum of services to assist our customers in realizing efficiencies, cost savings and freeing up much needed government resources. As subject matter experts in electronic monitoring supervision and reentry, her team takes a consultative approach to account management to ensure that the design of the program is in line with the goals of the agency. Additionally, this team utilizes their experience in the industry and their relationships with our customers to introduce advanced technologies and services into existing programs to grow brand loyalty and revenue through a spectrum of services offering.

Mrs. Starr began her career in the electronic monitoring industry in 1997, 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 the Western Region where she was responsible for all branch operations and business development in 12 states. In 2010, Mrs. Starr accepted an opportunity to become Vice President of Customer Service with an industry manufacturer. For four (4) years she gained valuable senior leadership experience and managed staff and accounts both domestically and abroad. In 2014, Mrs. Starr returned to Sentinel as the Vice President of Field Operations and was promoted to Senior Vice President of Field Operations in 2018. Mrs. 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 web-based information 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 is responsible for retention, growth, strategy, budget development, forecasting and the P&L for all domestic accounts.

Mrs. Starr is fully trained in the current NASPO ValuePoint Agreement and will be trained again in the details of the next NASPO ValuePoint Master Agreement. In her role, Mrs. Starr will ensure her team is fully aware of the NASPO Master Agreement and trained in its effective utilization across the country.

BILL HECKER | Senior Regional Account Manager

Mr. Hecker has been involved in field operations for the electronic monitoring industry since 1999. He joined Sentinel in 2012. His responsibilities have continued to expand and today include project management, customer training, account management, and agency transition processes. Mr. Hecker provides on-going customer support and has proven instrumental to the success of several major agency programs due to his extensive experience with program implementation. Prior to joining Sentinel, Mr. Hecker worked for Sentencing Concepts, a provider of alternative sentencing services. He acted as a court liaison and installer and overall project director. He holds a bachelor's degree in Sociology from California State University, Long Beach, and an MBA from the University of Phoenix. For this program, Mr. Hecker will:

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Account retention;
- + Being the main liaison between the Customer and Sentinel;
- + Providing consultative account management practices to government channel accounts in his region to ensure best practices are in place;
- + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
- + Introduction and socialization of hardware and software offerings that may benefit the Customer;
- + Conducting training and overseeing the implementation; and
- + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.

DARIN SIMION | Senior Regional Account Manager

Mr. Simion's career began in 2004 working for Marion County Community Corrections (Indiana) as a field officer managing a caseload of 300 home detention and pretrial offenders. He has been involved in implementation and supervision of more than 35 agency-run monitoring programs nationwide. He has held several positions including Community Corrections Officer, Trainer, and Electronic Monitoring Specialist. He has extensive experience with authoring and delivery of agency training. In 2007, Mr. Simion joined the Sentinel team as a Regional Account Manager. He manages a portfolio of services that includes customer logistics, training, and consultancy. For this program, Mr. Simion will:

- + Account retention;
- + Being the main liaison between the Customer and Sentinel;
- + Providing consultative account management practices to government channel accounts in his region to ensure best practices are in place;
- + Making recommendations that foster workflow efficiencies and promote repeatable positive outcomes;
- + Introduction and socialization of hardware and software offerings that may benefit the Customer;
- + Conducting training and overseeing the implementation; and
- + Ensuring the scope of work as outlined in the service agreement is met by Sentinel.

DEDICATED SENTINEL ON-SITE TECHNICIANS

Sentinel is prepared to hire, train, and staff on-site personnel dedicated to the participating programs contracted under NASPO if required for program operations. These onsite employees can provide installations/removals as well as assist with enrollments, case management, troubleshooting, equipment maintenance and inventory, report generation and distribution, and collections. Sentinel's on-site technicians are available to provide a daily review of participant activity reports to determine the status of each participant's supervision on electronic monitoring. Based on each contracting agency's policies and procedures, Sentinel's technicians can also be available to contact participants to troubleshoot any equipment-related alerts. The technicians can be responsible for equipment inventory management, including all ordering of equipment and supplies as well as the return of excess inventory or devices in need of repair. The technicians can also be responsible for ensuring that all electronic monitoring equipment is properly cleaned and tested prior to placement upon each program participant.

Sentinel's technicians are well trained in the procedures associated with enrolling each participant and installing the equipment, including properly fitting the device to the participant's leg and taking enrollment photos for use with alcohol monitoring equipment. During the installation, the technician will instruct the participant on the care and daily maintenance of the equipment as well as instruct the participant on proper charging requirements and testing procedures. Upon completion of the installation, the technician will ensure that all signals from the equipment are received within the monitoring platform prior to allowing the participant to exit the facility. In addition, depending on the contracting agency's requirements, our on-site technician can be responsible for the following tasks:

- + Assessment and collection of program fees from participants;
- + Be available to provide court testimony as needed;

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



- + Be available to troubleshoot key events/alerts with officers to ensure accuracy and certainty;
- + Handle all shipping, receiving, cleaning, and testing of equipment on behalf of the Agency.
- + Assist in equipment recovery and inventory reporting in compliance with Agency's and Sentinel's protocols.
- + Provide analysis and recommendations or alternatives to issues and problems to address any concerns in order to be more efficient;
- + Enter monitoring demographics into Sentinel's automated system prior to the installation of monitoring equipment;
- + Meet the fulfillment requirement that installation and removal of equipment and service are completed within the timelines required; and
- + Meet the fulfillment of maintenance or troubleshooting as necessary and respond and provide resolution within 24 hours to ensure program continuity.

MYRIAM MONTALVO-SUNGA | Director of Logistics Operations

Mrs. Montalvo-Sunga joined Sentinel in 2016 and has held various roles in Sentinel's National Monitoring Center during her tenure. As Help Desk Supervisor, she was responsible for Tier-1 customer support delivery, supervising a team of seven (7) technicians, driving changes and results related to ISO certification maintenance, and identifying trends involving product and system performance. Prior to Mrs. Montalvo-Sunga's appointment as Help Desk Supervisor, she was a Help Desk Lead and responsible for Help Desk personnel performance, investigating and reporting abnormalities with Sentinel's products and Services, and delivering operational efficiencies. She earned her Bachelor of Arts degree from the University of California at Los Angeles in 2014.

In December of 2024, Mrs. Montalvo-Sunga was promoted to Director Logistics Operations. In her new role, she oversees the full life cycle of Sentinel's assigned products by managing the assembly, repairs, warehousing, and disposal of electronic monitoring devices and related accessories, and processing the procurement, distribution, allocation, and delivery based on contract terms and corporate planning. She analyzes and coordinates logistical operations, including raw materials, production, equipment repairs, consumables, and fixed asset inventories, to ensure efficient and cost-effective supply chain management across the product lines and organization. As Director of Logistics Operations, Mrs. Montalvo-Sunga is primarily responsible for:

- + Leading Sentinel's Equipment Services, Fulfillment, and Warehouse teams.
- + Overseeing company operations related to the acquisition, repair, distribution, warehousing, and disposal of raw materials, consumables, and fixed assets.
- + Supervision physical inventory count operations as scheduled by the Finance Department, external auditors, or management.
- + Managing third party relationships including contract manufacturers, equipment repair centers, and suppliers of electronic monitoring equipment and consumables.
- + Planning, organizing, and executing logistics support activities such as maintenance planning, repair (RMA) analysis, and test equipment requirements.
- + Delivering efficient and cost-effective supply chain management and operational efficiencies.

CHRISTY SUAZO | National Service Center Director and Custodian of Records

Mrs. Suazo has been involved in internal operations for the electronic monitoring industry since 2009. Mrs. Suazo began her electronic monitoring career with G4S Judicial Services as a Dispatcher, Monitoring Center Operator, and a Help Desk Technician. In 2012, she joined the Sentinel team, and her responsibilities have continued to expand and have included roles as Help Desk Supervisor, Monitoring Center Manager, and now as National Service Center Director, overseeing Sentinel's Monitoring Center and Help Desk operations, as well as Custodian of Records since 2018. As part of Mrs. Suazo's regular duties, she maintains custody and control of the original records of Sentinel Offender Services, LLC. Mrs. Suazo is required to attest to the truth and accuracy of the records that can include but are not limited to the original memorandums, reports, records, data compilations or other business records maintained by Sentinel as regular practice in the course of the regularly conducted



activities of Sentinel.

As the National Service Center Director, Mrs. Suazo is responsible for the day-to-day supervision and management of the National Monitoring Center and other functional departments. As a member of the Operations management team, Mrs. Suazo participates in the strategic planning process, develops and manages budgets, implements and manages organizational change, and determines the financial impact of management decisions. In addition, she is responsible for leading the National Service Center team to ensure that all terms and conditions of Sentinel customer contracts are met. In this capacity, she assists in the successful resolution of difficult and/or complex customer issues or problems that have been escalated. Mrs. Suazo's primary duties and responsibilities include:

- + Developing, managing, motivating and leading a customer service team to create a definitive value-add for our customers (internal and external) and a distinct differentiator from our competition. Initiating recruitment and development programs that establish team members as experts in our industry and ensuring that they are perceived as such by all Sentinel customers.
- + Establishing, investigating and resolving issues while producing timely management reports related to Key Performance Indicators (KPI) for assigned areas of responsibility and related positions. Identifying trends, patterns, and priorities relating to Key Performance Indicators and other performance measurements.
- + Identifying and mitigating any risks relating to the monitoring of financial service operations and equipment.
- + Designing collection programs that permit Sentinel employees to effectively collect outstanding fines, fees, and restitution from program participants. Reviewing records to identify delinquent account records that require collection action.
- + Supervising and coordinating the activities of employees engaged in collecting fines, fees, and restitution from program participants. Creating and managing spreadsheets/management information showing the progress of collection activities.
- + Developing, implementing, monitoring, and testing appropriate processes to facilitate contract compliance and customer satisfaction.
- + Identifying and implementing policies and procedures to improve the quality and efficiency of Sentinel's 24/7/365 National Service Center delivery of service to customers.
- + Proactively monitoring and managing communication routes between the customer and assigned internal or external operational contacts thereby ensuring that service is compliant with contractual obligations.
- + Diagnosing, resolving, or escalating advanced electronic monitoring hardware and software issues while staying current with technological trends related to hardware and software applications offered by Sentinel. Staying abreast of current news, system information, problems, changes and updates relevant to our internal and external user community.
- + Responding to internal and external customer requests via telephone, email, via remote access or in-person in a timely and professional manner.

DENNIS POTTS | Training Manager

Mr. Potts has been employed at Sentinel since May of 2023, and, since his hiring, has served as Compliance Manager in the Quality Assurance Department. Prior to joining Sentinel, Mr. Potts worked for Harris County Pretrial Services (Houston, Texas) for 32 years where he worked in the jails and in information technology for nine (9) years before serving as the agency's Deputy Director for 23 years. In the latter role, he was responsible for budget and policy development, vendor contracts and relationships, and facility oversight. Prior to working for Harris County, Mr. Potts served as a Parole Caseworker with the Texas Board of Pardons and Paroles, as a Probation and Parole Agent/Adult with the Louisiana Department of Public Safety and Corrections, and as a state university police officer.



In his current role as Training Manager, Mr. Potts is responsible for the organization and development of training related to Sentinel's hardware, services, and software platforms. He also is responsible for oversight of Sentinel's training staff, who provide training for Sentinel employees and customers.

Mr. Potts holds a Bachelor of Criminal Justice degree from Louisiana State University and a graduate degree in Human Relations and Supervision from Louisiana Tech University. While employed with Harris County, Mr. Potts served for several years as an adjunct Criminal Justice instructor and co-authored several published articles and book chapters on criminal justice topics. He also served as a Board Member of the National Association of Pretrial Services Agencies, and as a National Institute of Justice Special Technical Committee Member in the development of standards for offender tracking systems.

CONTINUOUS MONITORING CENTER OPERATIONS AND SUPPORT

Sentinel's National Monitoring Centers will continue to serve as the focal point for monitoring of participants on behalf of Participating Entities.

—IMPORTANT SENTINEL ADVANTAGE—

All of Sentinel's technologies and services proposed herein are monitored directly by Sentinel's own monitoring centers that are operational 24 hours a day, 7 days a week, 365 days a year. Sentinel owns, staffs, and operates both our Primary Monitoring Center and Secondary Monitoring Center.

Our monitoring centers are staffed 24 hours a day, 7 days a week, 365 days a year with a supervisor always on duty and operators *cross-trained to support our suite of supervision services and products*. Agency staff can call and speak with one of our monitoring experts at all times of the day or night. We currently employ more than 60 personnel to staff our continuous operations (24/7) facility. Staffing patterns include overlaps so that we have increased staff during the high-volume hours of each time zone. This staffing pattern permits us to process alarms during these peak periods without delays. In addition, our center is staffed with *bilingual personnel on every shift* to ensure successful interactions with program participants since operational protocols often require that our monitoring center directly contact program participants when certain alarms occur, regardless of the day of the week or time of the event.

—IMPORTANT SENTINEL ADVANTAGE—

In concert with evidence-based practices, Sentinel measures and reviews each process to determine effective outcomes. Similarly, we have demonstrated our commitment to quality processes by achieving the **ISO certification for our Manufacturing Facility for Production of Electronic Monitoring Equipment plus our Monitoring Center for the Provision of Electronic Monitoring Services**. This quality certification ensures that documented procedures are in place for all aspects of services performed by Sentinel's monitoring centers that are audited on a routine basis.

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

FINANCE AND ACCOUNTING

Sentinel's accounting team will continue to be led by Chief Financial Officer Dennis Fuller. To ensure seamless compliance, Mr. Fuller will be supported by Marcie Avalos and Marisol Greenburg—both of whom bring over a decade of experience with the NASPO ValuePoint Master Agreement. This team is responsible for the precise reporting and distribution of funds to NASPO ValuePoint. Additionally, Sentinel maintains a deep bench of Finance resources to provide additional support as needed as the number of Participating Entities expands.



6. Describe how you intend to encourage adoption and usage of your Master Agreement by Participating and Purchasing Entities.

SENTINEL RESPONSE

Sentinel has and will continue to promote the adoption of the NASPO ValuePoint Master Agreement as our preferred cooperative agreement through rigorous sales and marketing campaigns. As we have done for more than 25 years, Sentinel will use every opportunity to convert new and existing customers to the Master Agreement. Sentinel will continue to meet with Participating and Purchasing entities to ensure they are fully educated on the benefits, including cost savings, procurement efficiencies, and ease of use provided by the Master Agreement. Moreover, Sentinel will implement the strategies outlined in our response to Question #3 above where we will utilize our Sales and Marketing Department, Salesforce CRM, and Sentinel Account Managers to continually champion the NASPO Master Agreement. To summarize we will:

- + Maintain a landing page on the Sentinel corporate website specifically for the NASPO ValuePoint contract.
- + Launch a comprehensive, user-centric website designed in collaboration with NASPO ValuePoint to serve as a primary resource for all Participating Entities.
- + Utilize our Salesforce CRM, and Sentinel's Marketing and Inside Sales teams will execute targeted outreach campaigns utilizing email, LinkedIn, and social media efforts.
- + Advocate for NASPO ValuePoint and educate potential customers on the pre-vetted nature of the contract, which reduces the need for lengthy individual RFPs.
- + Guide potential entities through the exact steps required to join, from initial interest to the signing of a Participating Addendum.
- + Include a dedicated NASPO ValuePoint mention in agency-facing presentations to ensure the Master Agreement is always front-of-mind.

Sentinel's approach to encourage adoption and usage of our Master Agreement by Participating Entities includes advocating the following key benefits:

- + Breadth of Solutions available
- + Value via Volume-Based Prices
- + Length of Initial Term plus optional Renewal Terms
- + Provision of a Sample Participating Addendum with emphasis regarding Sentinel's willingness to incorporate the entity's own Terms & Conditions taking precedence

7. Describe your approach to negotiation of Participating Addenda. Describe the extent to which you will provide Participating Entities flexibility in incorporating entity-specific language into their Participating Addenda. (e.g., Do you require entities to provide statutory citations for their entity-specific language? Are you able to devote resources to simultaneous negotiation of multiple Participating Addenda?)

SENTINEL RESPONSE

Sentinel has and will continue to exercise flexibility in negotiating and executing Purchasing Addendums. Our goal is to make the Participating Addendum process as simple as possible, yet effective for the Participating Entity including incorporating required Participating Procurement Entity standard language. Sentinel does not require statutory citations for entity specific language. We believe we have demonstrated our ability to effectively execute NASPO Participating Addendums over our 25-year tenure with NASPO and we look forward to executing many more in the future.



Sentinel can negotiate Participating Addendums simultaneously as every member of our sales team, including our SVP of Sales and COO, are trained on the NASPO Master Agreement Purchasing Addendum Processes.

Sentinel's approach to negotiating Participating Addenda includes the provision of a Sample Participating Addendum with emphasis regarding Sentinel's willingness to incorporate the entity's own Terms & Conditions taking precedence.

Sentinel's entire Sales Team is fully experienced at promoting the Sentinel/NASPO Master Agreement and negotiating Participating Addenda, thus Sentinel already has the resources and expertise in place for simultaneous negotiation of multiple Participating Addenda.

8. Describe your ability to provide products and services immediately upon execution of a Master Agreement and Participating Addenda.

SENTINEL RESPONSE

As an incumbent vendor in all approved categories on NASPO ValuePoint Master Agreement #22PSX0021, Sentinel services will remain uninterrupted as updated Purchasing Addendums are executed with existing NASPO ValuePoint Entities.

For new Participating Entities executing a Participating Addendum Sentinel can implement program operations in accordance with Participating Entity requirements. Sentinel maintains available equipment inventory in both of our Regional Distribution Centers that can be shipped within 24 hours of notice. Our training department and Regional Account Managers can provide initial training on short notice, and when necessary, our staff can be on-site to begin program transition in less than 72 hours.

While Sentinel possesses the ability to implement new programs on short notice, it has been our experience that new Entities prefer a program transition that occurs over a period of 30 – 45 days, dependent on Entity needs.

ON-BOARDING

Sentinel's customer on-boarding is the strategic process of guiding new Participating Entities through introduction of Sentinel resource contacts and the initial setup, training, and transition of the products and services to help them achieve their first "win" and value realization with the emphasis aiming to build confidence, improve efficiency, and establish long-term, productive relationships.

Following mutual authorization of the Participating Addendum, Sentinel works with the Participating Entity to finalize an On-Boarding Work Plan and Timeline that includes all known contacts, tasks, deliverables, milestones, and duration estimates for each task and resource loading for the duration of the project. We understand the importance of open and fully transparent operations in the provision of public safety solutions and believe it is essential to the effective operation of any electronic monitoring program. We meet with Participating Entity personnel weekly during the initial implementation stages to review progress, performance, and to identify and resolve any programmatic challenges.

After mobilization, Sentinel continues to meet with the Participating Entity as necessary monthly or quarterly depending on the needs of each Participating Entity. We continue to provide all written reports to the Participating Entity as needed to operate an efficient and effective program including participant activity reports for each program participant and monthly summary reports. In addition, the Sentinel Regional Account Manager continues to always be available through telephone and/or email communications to address concerns or resolve issues with the program.

We work closely with the Participating Entity to ensure all needs, including implementation timeline expectations, are met during implementation and transition. We are highly flexible in our capability for mobilization and adjust

**Request for Proposals for
ELECTRONIC MONITORING**

Issued by the **State of Nevada**
Solicitation Number 99SWC-S3474



our plans and staffing requirements as needed per the decisions mutually agreed in the Initial Project Briefing and Information Session. The following is an example of the elements involved in Sentinel's On-Boarding Process:

On-Boarding Work Plan Milestone	Week 1	Week 2	Week 3	Week 4	Monthly Beginning at Program Start
Initial Project Briefing and Information Session: • Introduction of Sentinel Resource Contacts (Sales, Account Manager, Monitoring Center, Help Desk, Accounting/Billing) • Networking with other Sentinel Participating Entities for sharing Programmatic Policies and Best Practices • Confirmation/Schedule of Initial Order(s), Training and Transition • Agency Notification Profiling, what assistance, if any does the entity need with transferring existing program participants demographic data into Sentinel's Monitoring Application					
Pre-Production Project Evaluation and Analysis					
Design, Development and Testing					
On-site Program Staff Installation and Training					
Equipment Delivery					
Department Training					
Participant Enrollment & Equipment Transition					
Operation and Maintenance					
Assessment of Initial Order Fulfilment					
Ongoing Contract Monitoring and Reporting					

Sentinel promotes the Master Agreement to complete initial deliveries within approximately thirty (30) days from receipt of a fully authorized Participating Addendum. It is important to note that Sentinel, as the prime contractor for any contracted services performed, maintains both a Primary National Warehouse at our Corporate Headquarters in Anaheim, California as well as a Secondary National Warehouse located at 1005 Alderman Drive, Suite 108, Alpharetta, Georgia (30005). **With operations on both coasts, we can be of service and provide quicker equipment shipments to our customers.**



9. Describe how you will ensure summary and detailed sales information is promptly, completely, and accurately reported to you by your dealers, partners, and resellers for aggregation and reporting to NASPO ValuePoint in compliance with the terms of your Master Agreement.

SENTINEL RESPONSE

Sentinel will continue to ensure accuracy of the reported sales information through our internal accounting and Statement of Work processes. The Sentinel Accounting team is provided with read-only access to the monitoring system utilized by user Entities, dealers, partners and resellers for the provision of electronic monitoring services. This access allows our accounting team to identify and verify the actual number of monitoring devices, days monitored, start date, end date, and device type for each agency. Every reported sale is validated against our Salesforce CRM where all of the Participating Addendums are housed and the specific terms, discounts, and administrative fee structures of the relevant Purchasing Addendum are verified to ensure each identified user Entity is identified and properly reported.

The Sentinel accounting team members responsible for the NASPO ValuePoint sales reporting have been providing reports for more than 10 years, have become efficient in the process and will continue to be valuable resources in our delivery of quality reporting.

Sentinel already has the NASPO reporting processes and procedures in place as well as a dedicated Accounting contact responsible for administering summary and detailed sales information promptly, completely, and accurately for both NASPO as well as those Participating Entities with independent reporting requirements and/or independent administrative fees. It is also important to note that the individual currently in this dedicated Accounting contact role has been in place for fourteen (14) years and is intimately familiar with NASPO ValuePoint Master Agreements.



SUPPORTING DOCUMENTATION

Sentinel has provided the following supporting documentation as a supplement to this section of this Attachment:

- + **Letter of Support from SCRAM Systems (page 341)**
- + **Letter of Support from Shadowtrack Technologies (page 342)**
- + **International Organization of Standardization 9001:2015 Certificate (page 343)**
- + **Federal Communications Commission Certificates (page 346)**
- + **Service Level Agreement | Category 1: GPS (page 361)**
- + **Service Level Agreement | Category 2: RF (page 375)**
- + **Service Level Agreement | Category 3: Alcohol Monitoring (page 384)**
- + **Product and Service Brochures (page 395)**

National Association of State Procurement Officials (NASPO) ValuePoint

Dear Members of the Evaluation Committee,

I am writing on behalf of **SCRAM Systems** to formally express our full support for **Sentinel's response to the NASPO ValuePoint Request for Proposals for Electronic Monitoring**, issued by the **State of Nevada as the Lead State**.

SCRAM Systems and Sentinel have established a robust, secure, and proven technical integration that enables Sentinel's electronic monitoring hardware to operate seamlessly within SCRAM's software platform. This integration is designed to support the comprehensive electronic monitoring solutions contemplated under the NASPO ValuePoint Scope of Work, including but not limited to GPS monitoring, data management, reporting, system interoperability, and secure information handling.

Our integrated solution aligns with the cooperative purchasing framework established by NASPO ValuePoint and is built to scale across Participating Entities while maintaining consistent performance, reliability, and compliance with applicable federal, state, and local requirements. SCRAM Systems' software capabilities, combined with Sentinel's monitoring hardware, provide Participating Entities with a unified and efficient monitoring ecosystem that supports operational flexibility and long-term program success.

SCRAM Systems fully supports Sentinel's participation in this solicitation and believes that the combined strengths of our organizations will deliver significant value to the State of Nevada and all NASPO ValuePoint Participating Entities seeking secure, reliable, and court-validated electronic monitoring solutions.

We appreciate the opportunity to support Sentinel's response to this RFP and remain committed to continued collaboration in support of NASPO ValuePoint and its participating states.

Should you require any additional information or clarification, please do not hesitate to contact me directly.

Sincerely,



John Hennessey
Chief Operating Officer
SCRAM Systems

January 29, 2026

RE: National Association of State Procurement Officials (NASPO) ValuePoint - Sentinel Offender Services, LLC Letter of Certification

Dear Members of the Evaluation Committee,

The purpose of this letter is to document, confirm, and formally express that Shadowtrack Technologies Inc. recognizes Sentinel Offender Services LLC (Sentinel) as an authorized reseller, a premier business partner, and a value-added service provider authorized to sell Shadowtrack Technologies Inc.'s full continuum of advanced Monitoring Solutions.

Sentinel has full access to our latest generation of monitoring solutions and our complete support in offering these services in response to the NASPO ValuePoint Request for Proposals for Electronic Monitoring, issued by the State of Nevada as the Lead State.

Shadowtrack Technologies Inc. fully supports Sentinel's participation in this solicitation and believes that the combined strengths of our organizations will deliver significant value to the State of Nevada and all NASPO ValuePoint Participating Entities seeking secure, dependable, and reliable electronic monitoring solutions.

Should you want to speak with Shadowtrack Technologies Inc. about our partnership with Sentinel, please contact me directly.

Sincerely,



Robert Magaletta
CEO ShadowTrack Technologies Inc.





CERTIFICATE OF REGISTRATION

The management system of certificate number **266659**

Sentinel Offender Services, LLC

1220 Simon Circle, Unit C, Anaheim, CA, 92806, USA

has been assessed and certified as meeting the requirements of:

ISO 9001:2015

Design, Production, and Delivery of Electronic Monitoring Technologies, Monitoring Center Services, and Community Based Offender Management Programs

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.



Initial certification: Sunday, September 19, 2010

Current cycle start: Thursday, February 13, 2025

Latest issue: Tuesday, November 26, 2024

Expiry date: Saturday, February 12, 2028
Subject to annual assessments.



Certification structure: Multi Site

Authorized by

Mike Tims
Chief Executive Officer

amtivo.us

Certificate issued by Amtivo (USA) Inc.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo (USA) Inc, 7502 W. 80th Avenue, STE. 225 Arvada, Colorado 80003-2128, USA.



Expiry Date: **Saturday, February 12, 2028**

Certificate Number **266659**

Locations covered under certification:

- **Sentinel Offender Services, LLC (Overall Certification)**
1220 Simon Circle, Unit C, Anaheim, CA, 92806, USA
Design, Production, and Delivery of Electronic Monitoring Technologies, Monitoring Center Services, and Community Based Offender Management Programs
- **Sentinel Offender Services, LLC - Caldwell**
405 E. Elm Street, Caldwell, ID, 83605, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Dallas**
133 N. Riverfront Blvd 1st Floor Room A9, Dallas, TX, 75207, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Greenville**
101 Broadus Avenue, Greenville, SC, 29601, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Oroville**
51 County Center Drive, Oroville, CA, 95965, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Phoenix**
3806 N. 3rd St. Suite #200, Phoenix, AZ, 85012, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Riverside**
4133 10th St, Riverside, CA, 92501, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - San Diego**
7857 Convoy Court, Suite 201, San Diego, California, 92111, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - San Francisco**
70 Oak Grove, San Francisco, CA, 94170, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs
- **Sentinel Offender Services, LLC - Seattle**
600 5th Avenue, 8th Floor, Seattle, WA, 98104, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs

amtivo.us

Certificate issued by Amtivo (USA) Inc.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo (USA) Inc, 7502 W. 80th Avenue, STE. 225 Arvada, Colorado 80003-2128, USA.



Expiry Date: **Saturday, February 12, 2028**

Certificate Number **266659**

Locations covered under certification:

- **Sentinel Offender Services, LLC (Overall Certification)**
1220 Simon Circle, Unit C, Anaheim, CA, 92806, USA
Design, Production, and Delivery of Electronic Monitoring Technologies, Monitoring Center Services, and Community Based Offender Management Programs
- **Sentinel Offender Services, LLC - Tacoma**
930 Tacoma Avenue South, Room 136, Tacoma, WA, 98402, USA
Location Scope: Delivery of Electronic Monitoring Technologies, Case Management Services, and Community Management Programs

amtivo.us

Certificate issued by Amtivo (USA) Inc.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo (USA) Inc, 7502 W. 80th Avenue, STE. 225 Arvada, Colorado 80003-2128, USA.

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Timco Engineering, Inc.
849 NW State Road 45
Newberry, FL 32669

Date of Grant: 10/04/2018

Application Dated: 09/10/2018

Sendum Wireless Corp.
4500 Beedie Street
Burnaby, V5J5L2
Canada

Attention: Henry Seto , Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
VALID ONLY for the equipment identified hereon for use under the Commission's
Rules and Regulations listed below.

FCC IDENTIFIER: TS5-WP76-OM500
Name of Grantee: Sendum Wireless Corp.
Equipment Class: Licensed Non-Broadcast Station
Transmitter
Notes: Digital Transceiver Ankle

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
BC	27	1720.0 - 1745.0	0.132	2.5 PM	17M9G7D
BC	27	1720.0 - 1745.0	0.125	2.5 PM	17M9W7D
BC	27	779.5 - 784.5	0.169	2.5 PM	4M53G7D
BC	27	782.0 - 782.0	0.164	2.5 PM	8M88G7D
BC	27	782.0 - 782.0	0.141	2.5 PM	8M88W7D

Output Power is EIRP and ERP for above and below 1 GHz, respectively. This device
supports LTE of 1.4, 3, 5, 10, 15, and 20 MHz bandwidth modes for FDD LTE Band 4; and
LTE of 5, and 10MHz bandwidth modes for FDD LTE Band 13.

BC: The output power is continuously variable from the value listed in this entry to 5%-10% of the value listed.

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Timco Engineering, Inc.
849 NW State Road 45
Newberry, FL 32669

Date of Grant: 04/22/2022

Application Dated: 04/22/2022

Sendum Wireless Corp.
4500 Beedie Street
Burnaby, V5J5L2
Canada

Attention: Henry Seto , Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
VALID ONLY for the equipment identified hereon for use under the Commission's Rules
and Regulations listed below.

FCC IDENTIFIER: TS5-OM500B
Name of Grantee: Sendum Wireless Corp.
Equipment Class: Part 15 Class B Digital Device
Notes: Digital Transceiver

Grant Notes

FCC Rule Parts
15B

Frequency
Range (MHZ)

Output
Watts

Frequency
Tolerance

Emission
Designator



Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Ultratech Engineering Labs Inc.
3000 Bristol Circle
Oakville (Ontario), L6H 6G4
Canada

Date of Grant: 12/10/2008
Application Dated: 12/10/2008

G4S Justice Services Canada, Inc.
#103 - 6592, 176 Street
Surrey, V3S 4G5
Canada

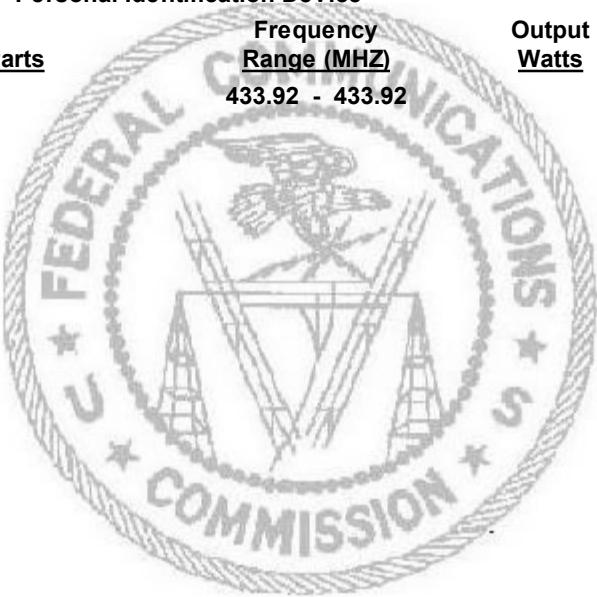
Attention: Harv Hundal , Software Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: NSNPTX08
Name of Grantee: G4S Justice Services Canada, Inc.
Equipment Class: Part 15 Remote Control/Security Device Transceiver
Notes: Personal Identification Device

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15.231(e)	433.92 - 433.92			



Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Ultratech Engineering Labs Inc.
3000 Bristol Circle
Oakville (Ontario), L6H 6G4
Canada

Date of Grant: 12/08/2008
Application Dated: 12/08/2008

G4S Justice Services Canada, Inc.
#103 - 6592, 176 Street
Surrey, V3S 4G5
Canada

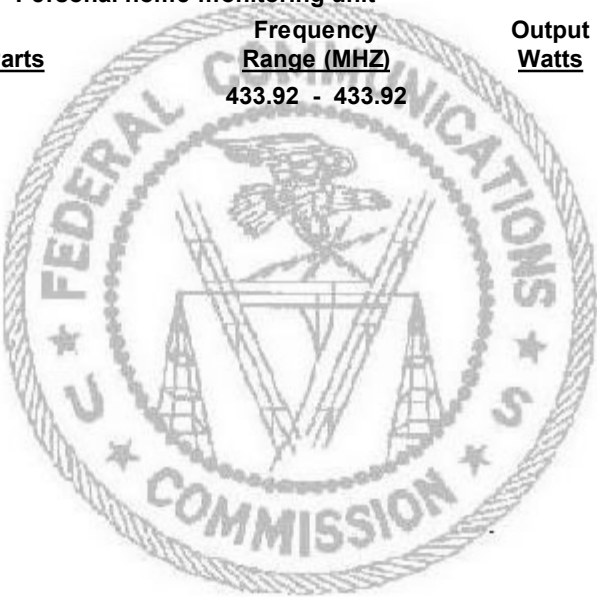
Attention: Harv Hundal , Software Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: NSNPHMUC08
Name of Grantee: G4S Justice Services Canada, Inc.
Equipment Class: Part 15 Remote Control/Security Device Transceiver
Notes: Personal home monitoring unit

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15.231	433.92 - 433.92			



Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Ultratech Engineering Labs Inc.
3000 Bristol Circle
Oakville (Ontario), L6H 6G4
Canada

Date of Grant: 12/11/2008
Application Dated: 12/11/2008

G4S Justice Services Canada, Inc.
#103 - 6592, 176 Street
Surrey, V3S 4G5
Canada

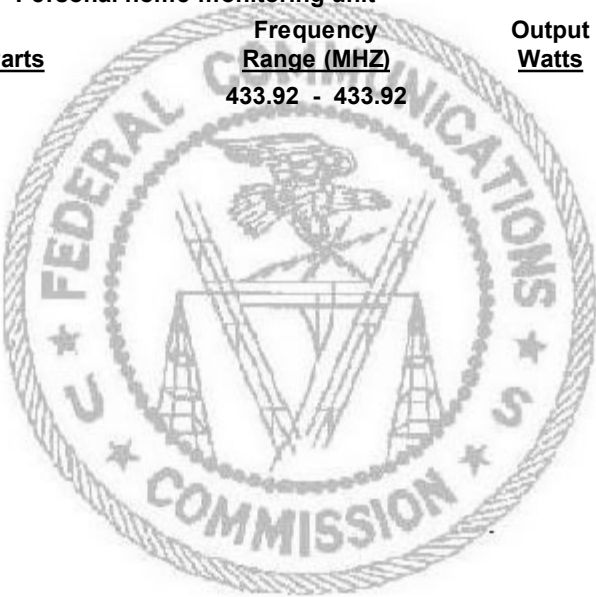
Attention: Harv Hundal , Software Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY
for the equipment identified hereon for use under the Commission's Rules and Regulations listed
below.

FCC IDENTIFIER: NSNPHMUL08
Name of Grantee: G4S Justice Services Canada, Inc.
Equipment Class: Part 15 Remote Control/Security Device Transceiver
Notes: Personal home monitoring unit

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15.231	433.92 - 433.92			



Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Ultratech Engineering Labs Inc.
3000 Bristol Circle
Oakville (Ontario), L6H 6G4
Canada

Date of Grant: 12/08/2008
Application Dated: 12/08/2008

G4S Justice Services Canada, Inc.
#103 - 6592, 176 Street
Surrey, V3S 4G5
Canada

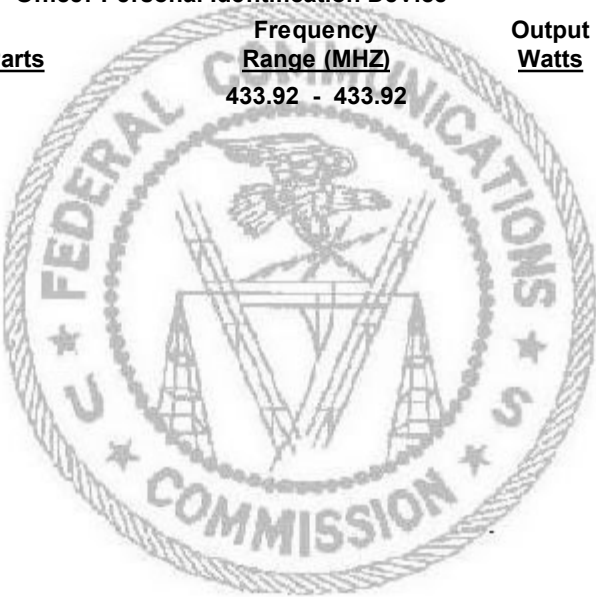
Attention: Harv Hundal , Software Engineer

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY
for the equipment identified hereon for use under the Commission's Rules and Regulations listed
below.

FCC IDENTIFIER: NSNOPID08
Name of Grantee: G4S Justice Services Canada, Inc.
Equipment Class: Part 15 Remote Control/Security Device Transceiver
Notes: Officer Personal Identification Device

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15.231(e)	433.92 - 433.92			



TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 12/21/2007
Application Dated: 12/21/2007

Alcohol Monitoring Systems LLC,
9135 S. Ridgeline Blvd.
Suite #190
Highlands Ranch, CO 80129

Attention: Jeff Hawthorne , Vice President of Research & Development

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and
is VALID ONLY for the equipment identified hereon for use under the
Commission's Rules and Regulations listed below.

FCC IDENTIFIER: P8M-SM02

Name of Grantee: Alcohol Monitoring Systems LLC

Equipment Class: Part 15 Low Power Communication Device
Transmitter

Notes: SCRAM II Bracelet

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	916.45 - 916.45			

The device must transmit with a source-based time-averaging duty factor not
exceeding 25 %



TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 10/23/2009
Application Dated: 10/23/2009

Alcohol Monitoring Systems LLC.
9135 S. Ridgeline Blvd.
Suite #190
Highlands Ranch, CO 80129

Attention: Jeff Hawthorne , Vice President of Research & Development

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and
is VALID ONLY for the equipment identified hereon for use under the
Commission's Rules and Regulations listed below.

FCC IDENTIFIER: P8M-SM03
Name of Grantee: Alcohol Monitoring Systems LLC.
Equipment Class: Part 15 Low Power Communication Device
Transmitter
Notes: SCRAM X Base Station

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	916.5 - 916.5			



PART 68 EQUIPMENT TCB CERTIFICATE

Certification under Part 68, Connection of Terminal Equipment to the Telephone Network

The product listed below has been found to comply with the applicable requirements for terminal equipment in accordance with the current editions of Federal Communications Commission CFR 47 Part 68, TIA-968-A-1, A-2, A-3, A-4, A-4, A-5, TIA-1096-A and TSB-168A as adopted by the Administrative Council for Terminal Attachments (ACTA).

Product No. US: AMSMM00BSM03
File Number: 3181176ATL-001 **Date of Grant:** August 31, 2009
Type of application: Original
Responsible Party: Alcohol Monitoring Systems
Country of origin: USA
Type of Equipment: Modem that connects to loop start modem.

Trade Name(s)
SCRAMx Base Station

Model Number(s)
AMS-SM03

AC REN: 0.0B DC REN: N/A Connectors: RJ11C

Authorized Network Port(s):

Service Order Codes(s):

- Telephone equipment containing Radio-Frequency circuitry may require additional equipment authorization(s) to be issued by the Commission prior to marketing such equipment in the United States. Failure to obtain the required equipment authorizations, when required, may subject the registrant to fines and penalties provided for in Table V, Section 501 and 503 of the Communications Act of 1934, as amended.
- Each piece of equipment bearing the bearing the listed trade name(s) and model number(s) listed above shall be labeled as specified in 47 C.F.R. Section 68.300(b) and TIA/EIA TSB 168.
- A copy of this certificate must be presented to U.S. Customs when any Foreign-Made Products identified herein are imported into the U.S.

The Telecommunication Certification Body listed below has been authorized by the FCC to issue this Equipment Certification. The equipment listed above has been shown to comply with the applicable Rules by the Responsible Party.

Name of TCB: Intertek Testing Services NA, Inc.
Address of TCB: 70 Codman Hill Road
Boxborough, MA 01719
Phone Number of TCB: 978-263-2662

Administrator e-mail: TCB_Admin@Intertek.com
Web site (URL) of TCB: www.etlsemko.com

Intertek

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

MiCOM Labs
575 Boulder Court
Pleasanton, CA 94566

Date of Grant: 08/12/2020

Application Dated: 08/12/2020

Alcohol Monitoring Systems Inc.
1241 W Mineral Ave
Suite #200
Littleton, CO 80120

Attention: Gordon Murray , Director of Engineering

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
 VALID ONLY for the equipment identified hereon for use under the Commission's Rules
 and Regulations listed below.

FCC IDENTIFIER: P8M-BS500
Name of Grantee: Alcohol Monitoring Systems Inc.
Equipment Class: Digital Transmission System
Notes: BS500

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
CC	15C	2412.0 - 2462.0	0.159		

Output power listed is conducted. This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with FCC multitransmitter product procedures. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

CC: This device is certified pursuant to two different Part 15 rules sections.

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 10/23/2009
Application Dated: 10/23/2009

Alcohol Monitoring Systems LLC,
9135 S. Ridgeline Blvd.
Suite #190
Highlands Ranch, CO 80129

Attention: Jeff Hawthorne , Vice President of Research & Development

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and
is VALID ONLY for the equipment identified hereon for use under the
Commission's Rules and Regulations listed below.

FCC IDENTIFIER: P8M-SM03

Name of Grantee: Alcohol Monitoring Systems LLC

Equipment Class: Part 15 Low Power Communication Device
Transmitter

Notes: SCRAM X Base Station

Grant Notes

FCC Rule Parts
15C

Frequency
Range (MHZ)
916.5 - 916.5

Output
Watts

Frequency
Tolerance

Emission
Designator



Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 05/23/2022

Application Dated: 05/19/2022

Alcohol Monitoring Systems Inc.
1241 W Mineral Ave
Suite #200
Littleton, CO 80120

Attention: Kyle Glavan , Director of Engineering

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
 VALID ONLY for the equipment identified hereon for use under the Commission's Rules
 and Regulations listed below.

FCC IDENTIFIER: P8M-RB200

Name of Grantee: Alcohol Monitoring Systems Inc.

Equipment Class: Part 15 Spread Spectrum Transmitter

Notes: Communication Module

Modular Type: Limited Single Modular

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
CC	15C	2402.0 - 2480.0	0.009		

Limited Modular Approval. Power listed is conducted. For professional installation only. Device shall not be sold to general public. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with FCC multi-transmitter product guidelines. Use in portable RF exposure conditions will require additional filing for SAR compliance. Compliance of this device in all final product configurations is the responsibility of the Grantee. This module can only be used with a host antenna circuit trace layout design in strict compliance with the OEM instructions provided. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

CC: This device is certified pursuant to two different Part 15 rules sections.

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 10/06/2022
Application Dated: 10/06/2022

Alcohol Monitoring Systems Inc.
1241 W Mineral Ave
Suite #200
Littleton, CO 80120

Attention: Kyle Glavan , Director of Engineering

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
VALID ONLY for the equipment identified hereon for use under the Commission's Rules
and Regulations listed below.

FCC IDENTIFIER: P8M-RB200

Name of Grantee: Alcohol Monitoring Systems Inc.

Equipment Class: Digital Transmission System

Notes: Communication Module

Modular Type: Limited Single Modular

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	2412.0 - 2462.0	0.115		

Limited Modular Approval. Power listed is conducted. For professional installation only. Device shall not be sold to general public. This change establishes portable category SAR conditions for the antenna and host described in this filing. The highest reported SAR for extremity (hand) exposure condition is 0.64 W/kg. Contains FCC ID: QIPTX62-W

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Intertek Testing Services NA, Inc.
70 Codman Hill Road
Boxborough, MA 01719

Date of Grant: 05/23/2022

Application Dated: 05/19/2022

Alcohol Monitoring Systems Inc.
1241 W Mineral Ave
Suite #200
Littleton, CO 80120

Attention: Kyle Glavan , Director of Engineering

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
 VALID ONLY for the equipment identified hereon for use under the Commission's Rules
 and Regulations listed below.

FCC IDENTIFIER: P8M-RB200

Name of Grantee: Alcohol Monitoring Systems Inc.

Equipment Class: Digital Transmission System

Notes: Communication Module

Modular Type: Limited Single Modular

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
CC	15C	2412.0 - 2462.0	0.174		
CC	15C	2402.0 - 2480.0	0.007		

Limited Modular Approval. Power listed is conducted. For professional installation only. Device shall not be sold to general public. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with FCC multi-transmitter product guidelines. Use in portable RF exposure conditions will require additional filing for SAR compliance. Compliance of this device in all final product configurations is the responsibility of the Grantee. This module can only be used with a host antenna circuit trace layout design in strict compliance with the OEM instructions provided. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

CC: This device is certified pursuant to two different Part 15 rules sections.

GRANT OF EQUIPMENT
AUTHORIZATION

Certification

Issued Under the Authority of the
Federal Communications Commission

By:

MiCOM Labs
575 Boulder Court
Pleasanton, CA 94566

Date of Grant: 09/12/2023
Application Dated: 09/07/2023

ShadowTrack Technologies, Inc.
5100 Village Walk
Suite 100
Covington, LA 70433

Attention: Robert Magaletta , President, CEO

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
VALID ONLY for the equipment identified hereon for use under the Commission's
Rules and Regulations listed below.

FCC IDENTIFIER: 2ARH7-W-N70ST
Name of Grantee: ShadowTrack Technologies, Inc.
Equipment Class: Part 15 Spread Spectrum Transmitter
Notes: ShadoWatch

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	2402.0 - 2480.0	0.0018		

Output power listed is conducted power.



Service Level Agreement – Category 1: GPS

SERVICE LEVEL AGREEMENTS

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements (“SLAs”).

PERFORMANCE OBJECTIVES

Sentinel has established standards that serve as minimum performance criteria throughout the company. These standards will not be enforced as contradictory to the orders of any customers but, rather, to ensure that Sentinel manages the offender monitoring process to the highest possible level of consistent professionalism possible. The Quality Management Team will routinely revise company standards as needed and publish these revisions through memos, emails, checklists and Standard Operating Procedure (SOP) changes. These company standards, regardless of the medium employed for communicating them, will be adhered to as the minimum standards for Sentinel and will be effective immediately as indicated.

Along with these Universal Standards a series of checklists and Key Performance Indicator Reports will be available to employees in all departments and/or at field offices for purposes of self-evaluating their compliance with standards both applicable to the company as well as their department/office. Where local differences may exist between the Universal Standards and the Participating Entity standards, the highest possible standard that does not conflict with the Participating Entity’s standards will be observed.

Global KPIs (key performance indicators) from Department Heads are collected to evaluate the performance and the effectiveness of the quality management system. Global KPIs captures performance metrics for the following Departments: Monitoring Center, Quality, Training, Human Resources, Production, and Technology. These Monthly reports will be made available to the Participating Entity upon request.

Sentinel collects data throughout our operation that allows us to effectively report on the significant metrics outlined in this section.

- 1) Our trained Equipment Service personnel record device RMA (return material authorization) evaluation results in Sentinel’s Home Inventory program. Daily Sentinel monitors devices return, along with the description of the malfunction and captures the root cause. These findings are reviewed monthly with senior management and corrective actions are implemented if device malfunction rates warrant. Monthly evaluation reports are available upon request to our customers.
- 2) Our Evaluation report captures return date, evaluation date, and repair completion date. This report demonstrates the responsiveness to issues and speed to resolution which Sentinel has implemented to resolve outstanding issues.
- 3) All devices returned are evaluated and tested to conform to Sentinel’s stringent FQC (final quality control) requirements to confirm that the unit is fully functional at the time of shipment. Moreover, all device maintenance is captured in Sentinel’s Home Inventory program to ensure device calibration and maintenance schedules are adhered to. Maintenance records are available to our customers upon request.
- 4) Local operating procedures are established at the agency level to ensure adherence to court-ordered schedules for installation and removal of Products and Services.
- 5) Sentinel works directly with the Participating Entity personnel to establish reporting protocols at the outset of the program. These protocols serve as the basis for monitoring response and performance measurement. These protocols establish the timeliness of response and report submittal requirements required by the Participating Entity.

- 6) Sentinel will provide complete transparency and results of our internal reporting. At the Participating Entities request we will complete the mandatory or specific government evaluation forms documenting our performance.
- 7) Training department periodically distributes a customer survey upon completion of training to improve customer training experience. Training survey includes questions regarding training knowledge and training material. Results of those satisfaction surveys will be provided to the Participating Entities upon request.
- 8) The Director of Quality Assurance periodically distributes an NPS Survey to all customers to improve overall service quality. The survey includes evaluation of all aspects of our operation including the Monitoring Center and Help Desk services. The results of these surveys provide guidance for our continual improvement efforts and results are available to our customers at any time.

SERVICE REQUESTS FROM PARTICIPATING ENTITY AND/OR PRODUCT USER

Sentinel responds to product and service request(s) from the User and Product User per the Participating Entity's Participating Addendum.

Sentinel is not responsible for Product User damage as defined as Product User misuse, neglect or abuse of an installed Product and/or Service, and Sentinel understands we retain the right to bill the Purchasing Entity and/or Product User at a fee schedule negotiated per the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

As an added benefit to Participating Entities, the Sentinel pricing proposed herein includes an annual volume of replacements for lost, damaged and/or stolen equipment equivalent to up to five percent (5%) of the units in active use on participants, at no additional cost. Lost, damaged and/or stolen replacement pricing proposed herein are for losses more than the included annual five percent (5%) replacements.

MAINTENANCE, SUPPORT AND SERVICING AGREEMENTS FOR PRODUCTS AND SERVICES

Sentinel understands and acknowledges that the Participating Entity may negotiate and incorporate into its Participating Addendum, product maintenance, support and/or servicing agreements for any products and/or Services purchased outright or rented by the Participating Entity.

Sentinel understands and acknowledges that, unless otherwise determined by the Participating Entity, pricing is based on a flat rate fee which at a minimum includes but is not limited to, contractor time and materials, and preventative maintenance. We understand and acknowledge that the term of such an agreement cannot exceed the useful life of the product(s) and/or services rendered as determined by either the Product and/or Service Manufacturer and/or the Participating Entity.

MAINTENANCE, SUPPORT AND SERVICING TECHNICIANS, PREVENTATIVE MAINTENANCE AND REPAIR PARTS AND SERVICE LOGS

Sentinel Employs Service Technicians for all OEM equipment.

Sentinel is the OEM or authorized distributor and as such the Service Technicians are properly trained and certified according to Sentinel's ISO Certification.

PREVENTATIVE MAINTENANCE & REPAIR PARTS

Sentinel performs all preventative maintenance services at the Product manufacturer's directed intervals, or as specified by a Participating Addendum.

Sentinel ensures all Product components, spare parts, and ancillary equipment that is supplied under the Master Agreement, will conform to manufacturer specifications including for use interfacing with proposed information technology solution(s).

Sentinel is responsible for ensuring that any repair parts are operable and installed in accordance with manufacturer specifications.

Sentinel ensures repair parts are new.

SERVICE LOGS

Sentinel maintains a digital record in the Repairs portal housed in Home Inventory System. This Repairs portal allows for a full history of all preventative maintenance and repairs performed on each piece of Monitoring Equipment.

Upon request, Sentinel provides digital service log(s) and/or requested information to the Participating Entity within three (3) calendar days of request.

PRODUCT AND SERVICE DELIVERY SPECIFICATIONS

For urgent orders and orders that require Priority Shipping, a Shipping Quote will be provided to the Participating Entity.

Sentinel understands and will provide a shipping quote prior to order placement from the Participating Entity for urgent orders that require priority shipping.

Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, California and Alpharetta, Georgia. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities.

All orders will ship within 1 Business Day of receipt and will be delivered FOB unless otherwise directed by the Participating Entity.

As appropriate, Sentinel can ship Product(s) overnight in emergency cases as deemed necessary by the Participating Entity and pursuant to the timeframes specified in the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

To minimize the emphasis on expedited shipments, Sentinel pricing proposed herein includes an on-site spare inventory of equipment equivalent to up to fifteen percent (15%) of the units in active use on participants, at no additional cost. Further, Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, California, and Alpharetta, Georgia. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities. Sentinel provides regular ground shipments to Participating Entities at no additional cost.

MONITORING SERVICES AND REQUIREMENTS FOR PRODUCTS AND SERVICES

Sentinel maintains monitoring center(s), within the United States. Sentinel's monitoring center(s) are equipped with redundant internet and telephone connectivity, as well as all other equipment required for

performance of all monitoring activities required pursuant to the proposed and awarded Products and Services under the Master Agreement.

Sentinel's datacenters are all located within the United States. All datacenters have uninterruptible power supplies and backup generators. The Primary facility in Los Angeles has backup internet service that can be used in the event of a major outage with the primary internet service. All critical components of Sentinel's Primary Information System are continuously replicated to our geographically redundant Secondary Information System in Dallas, Texas. Sentinel's Primary Information System is hosted on hardware maintained by Sentinel staff in a secure collocation facility in Los Angeles, California. The facility provides a full uninterruptible power supply (UPS), Generator, and redundant power circuit backups. Sentinel maintains separate AT&T and Sprint internet circuits in the Primary Information System for website and unit communication failover purposes. In the event of a disaster or failure, Sentinel can repoint websites and tracking unit communication to any provider or IP addresses to maintain the flow of traffic. Land Line traffic is provided by geo-redundant SIP trunks with Cox Communications with ability to failover to the Secondary Site automatically in the event of a failure.

Sentinel's Monitoring Center staff is decentralized and staffed across the United States so telephone impact due to a single location or entire geographic zone is minimized. Sentinel's primary National Monitoring Center is in our Norco, California, corporate facility and Sentinel's secondary Monitoring Center is in our Atlanta, Georgia, facility.

The cloud sections of Sentinel's application are deployed in reputed Oracle Government Cloud with primary services at Ashburn, Virginia and disaster recovery in Phoenix, Arizona. Both facilities have datacenter-grade hardware with redundant power supply and internet services.

The Sentinel monitoring center is available and staffed 24 hours a day, 7 days a week, 365 days a year through toll-free telephone and fax numbers to monitor Product User activity including activities in violation as defined by each respective Participating Entity's Participating Addendum. The monitoring operators and technicians are trained, experienced and capable of resolving most technical problems over the telephone or through remote diagnostics. In the unlikely event that problem solving requires a higher-level of involvement, Sentinel customer service is staffed by experienced technicians, each with diagnostic computer equipment to provide quick analysis and resolution of problems.

Databases are backed up offsite using Veeam to create and store 15-minute transaction logs, daily VM incremental snapshots, weekly synthetic full snapshots, and monthly active full backups.

Cloud databases are fully backed up weekly and incremental backup every 3 hours. Additionally, a standby database at the disaster recovery location is continuously synched down to 1 second.

Monthly, by the 5th business day of every month, the Director of QA produces a System Availability and Performance report that captures the System Availability and performance of the Hosted Services during the calendar month. Report includes:

- 1) System uptime percentage.
- 2) Incident details.
- 3) Root cause(s) and corrective action (s) to prevent recurrence
- 4) Sentinel makes these reports available to Participating Entities upon request.

PRODUCT USER MONITORING AND ACTIVITY REPORTS

The proposed Sentinel monitoring platforms provides customizable methods and parameters of violation notification to the Users and shall accommodate changes and customization at the Participating Entity's

request. The proposed Sentinel monitoring platforms provide methods for notification of Users and Product Users including immediate and next calendar day notifications via secure email, phone voice message, and cellular text message.

The proposed Sentinel monitoring platforms provide digital activity reports for all Products and Services deployed by the Participating Entity based on the required content specifications within the Participating Addendums.

Reports are available on the proposed Sentinel monitoring platforms via any web-enabled computer through the authorized user's login credentials (username and password). Reports are available on demand in standard format (Word, Excel, PDF), and Sentinel works with the Participating Entity to create customized reports.

Through the proposed Sentinel monitoring platforms, referring Users can enroll, terminate, modify, generate reports, add notes and otherwise perform Product User case activities through any internet-enabled device as well as by fax, email, and/or telephone.

Additionally, Sentinel's National Monitoring Center operators are available by fax, email, and/or telephone 24 hours a day, 7 days a week, 365 days a year to assist with enrollments, terminations, modifications, generating reports, adding notes, and otherwise assist with Product User case notes.

MONITORING SERVICE REQUIREMENTS

If Sentinel is authorized by a Participating Entity to invoice a Product User directly, the on-site Sentinel staff will establish in writing with Product User the fee schedule based on the policies and procedures established by the Participating Entity. Thereafter, for those program participants requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule established in writing with the Product User during their orientation.

Sentinel understands and will disclose information pertaining to how Product User data is collected and utilized by Sentinel or any subcontractor.

TRAINING REQUIREMENTS FOR USERS AND PRODUCT USERS

Customer training for Participating Entity authorized users is primarily coordinated by the Regional Account Manager (RAM) with Sentinel's Training Department. The Training Department will work together with the RAM to ensure each customer trainee has all the proper training documents (user guides, user manuals, PowerPoint presentations, reference guides, etc). Training is provided via in person training, virtual training sessions, and Instructor Led Training sessions (ILTs). For Product Users, installation guides, installation training videos, and ILTs are available upon request.

Sentinel training sessions are tailored to the Participating Entity's Category of Need. The Training Department will work together with the RAM to determine the Participating Entity's Category of Need and tailor the Training Agenda to the Participating Entity's needs as documented on the Customer's Training Attendance Log, including but not limited to, Operation of the Product and/or Service including any web-based information system, Installation, deactivation, removal and operation of Products and Services, Product and Service return processes and Other as specified by the Participating Entity. Customers can utilize our user-friendly RMA Request Form for Product and Services Return processes.

Sentinel's Training Department provides training as needed by the Participating Entity and will complete training within ten (10) calendar days of the request unless otherwise specified by the Participating Addendum. Sentinel requests as much advance notice as possible for in person on-site training so that travel arrangements can be made in advance.

Upon introduction of any new Product and Service feature, or whenever a user agency may need refresher training the Sentinel Training Department will make available user guides, user manuals, PowerPoint presentations, reference guides, training videos, and provide Instruction Led Trainings (ILTs) virtual trainings upon request, at no additional charge to the Participating Entity.

Sentinel makes digital training materials readily available upon request and provides unlimited access to on-line resources at no charge to the Participating Entity.

Sentinel provides a 24/7/365 toll free phone number and an email address for technical support. Participating Entities can contact Sentinel 24/7/365 at 800-589-6003 opt 2 or email Monitoring_center@sentineladvantage.com for customer support and receive an immediate response 24 hours per day.

SAMPLE GPS MONITORING NOTIFICATION PROTOCOL PROCEDURES

As part of on boarding with Participant Entities Sentinel works closely with the agency to set up Notification Protocol Procedures in our Monitoring Application. The following is a sample of a GPS program with Victim Notification Procedures being provided as an example of our Notification Protocol and flexibility to establish unique notification Protocol Procedures specific to the Participating Entities needs and requirements.

ALARM	ALARM RESPONSE	SCRIPT
LOW BATTERY	**Auto Clear Event: Charge On** 24/7 Step 1 - Role Based: Email Primary Officer Step 2 - Auto Email (Robocall): SE1464@TBD.com Step 3 - Delay: 20 min Step 4 - MC App <i>Instructions:</i> Call participant on all available numbers using script. If participant acknowledges script, input detailed notes then select CLOSE. If participant does not answer, leave a voicemail then input detailed notes and select CONTINUE. If participant refuses or is unable to charge, input detailed notes then select CONTINUE. Step 5 - Contact Victims <i>Instructions:</i> Call victim on all available numbers using script. Only call 911 if the victim does not feel safe and wants to implement emergency procedures. Input detailed notes then select Close.	<u>Script for Low Battery for Offender or VM</u> <i>"This is SENTINEL calling. You must charge your device for two continuous hours immediately. If you fail to charge your GPS device as instructed, your Family Relations Counselor & the local authorities will be notified."</i> <u>Script for Low Battery for Victim</u> <i>"Hello, this is SENTINEL calling for [victim's name]. We have received a Low Battery alert from [offender's name]'s GPS equipment which is still tracking."</i> If the offender was not contacted: "We have been unable to contact [offender's name]." If the offender refused: "The offender has refused to charge." If the offender is unable to charge immediately: "The offender is unable to charge immediately. Their last known location was [last known address] & they were moving [direction & approximate speed of movement if available]. I am providing this information so that if you feel the need you may implement your emergency procedures."
LOW BATTERY CLEAR	24/7 Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Check activity. If victim was NOT previously contacted for GPS Low Battery	

	alert, input notes then select CLOSE. If victim was contacted, call victim on all available numbers to inform them of clear. Input detailed notes then select Close.	
MEZ ENTERED	24/7 Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Continue. Step 3 - MC App <i>Instruction:</i> Call 911 for the city of the victim's current location using script. Input detailed notes then select Continue. Step 4 - Contact Victims <i>Instruction:</i> Check activity. If victim was already contacted, input notes then select CLOSE. If unsuccessful in contacting victim the first time, make a second attempt on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Close	Script for Mobile Exclusion Zone for Victim or VM <i>"Hello, this is SENTINEL calling for [victim's name]. Are you safe & can you freely speak, yes or no?"</i> If victim says no, immediately call 911 from a different line. If victim is free to speak ask for current location & continue: <i>"We have just received a mobile exclusion zone alert from [offender's name]'s GPS equipment indicating that the offender may be in your vicinity. Last known location was [last known address] & offender was moving [direction & approximate speed of movement if available]. I am providing this information so that if you feel the need you may implement your emergency procedures, which may include your calling 911. I will be calling 911."</i> Also, ask if victim would like you to remain on the phone while implementing emergency procedures. NOTE: If you remain on the line, call 911 from a different phone or have another operator call. Remain on the line & do not put the victim on hold if they do not feel safe or has implemented emergency procedures. Script for 911 <i>"Hello, this is a domestic violence offender alert on behalf of the insert agency name from SENTINEL regarding a protective order violation. We have just received a mobile exclusion zone alert from [offender's name]'s GPS equipment indicating that offender may be in the vicinity of the victim who is at [victim's last known location]. The offender's last known location was [last known address] & was moving [direction & approximate speed of movement if available]."</i> If the victim was successfully contacted include the following: <i>"I spoke to the victim, [victim's name], & victim's stated location is [reported location]."</i> If the victim was not contacted, include the following: <i>"I tried calling the victim [victim's name] cell phone & was not able to contact."</i> <i>"The offender, [offender's name], is a [gender, race, height, weight, hair color, eye color, & date of birth], & may be driving a [vehicle description]."</i> The 911 dispatcher may ask the Monitoring

		Center for additional information. After all requested information has been provided tell the dispatcher your name & telephone number & ask, "May I please have your name for our records?"
MEZ CLEARED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers to inform them of clear, using script. If no answer, leave a voicemail. Input detailed notes then select Close.	Script for Mobile Exclusion Zone Clear for Victim or VM <i>"Hello, this is SENTINEL calling for [victim's name]. "We have just received the clear for the mobile exclusion zone alert from [offender's name]'s GPS equipment indicating that the offender is no longer in your vicinity."</i>
MEZ BUFFER ENTERED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Close.	Script for Mobile Buffer Zone for Victim or VM <i>"Hello, this is SENTINEL calling for [victim's name]. We have just received a mobile buffer zone alert from [offender's name]'s GPS equipment indicating that he may be in your vicinity. Offender last known location was [last known address] & was moving [direction & approximate speed of movement if available]. I am providing this information so that you may implement your emergency procedures if you feel the need. We will continue to monitor the offender's location. If offender enters the mobile exclusion zone, you will again be contacted."</i> Ask for victim current location and whether to remain on the phone while implementing emergency procedures.
MEZ BUFFER CLEARED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers to inform them of clear, using script. Input detailed notes then select Close.	Script for Mobile Buffer Zone Clear for Victim or VM <i>"Hello, this is SENTINEL calling for [victim's name]. We have just received the clear for the mobile buffer zone alert from [offender's name]'s GPS equipment indicating that the offender is no longer in your vicinity."</i>
EXCLUSION ZONE ENTERED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Continue. Step 3 - MC App <i>Instruction:</i> Call 911 using script. Input detailed notes then select Continue. Step 4 - Contact Victims <i>Instruction:</i> Check activity. If victim was already contacted, input notes then select CLOSE . If unsuccessful in contacting victim the first time, make a second attempt on all available numbers using script. If no answer,	Script for Stationary Exclusion Zone for Victim or VM <i>"Hello, this is Sentinel calling for [victim's name]. Are you safe & can you freely speak, yes or no?"</i> If she says no, immediately call 911 from a different line. If victim is free to speak, ask for current location & continue: <i>"We have received a stationary exclusion zone alert from [offender's name]'s GPS equipment indicating that the offender may be in the vicinity off[zone address]. Offender last known location was [last known address] & was moving [direction & approximate speed of movement if available]. I am providing this information so that you may implement your</i>

	leave a voicemail. Input detailed notes then select Close.	<i>emergency procedures. I will be calling 911.</i>" Also, ask if victim would like you to remain on the phone while implementing emergency procedures. NOTE: If you remain on the line, call 911 from a different line. Remain on the line and do not put the victim on hold if he/she does not feel safe or has implemented emergency procedures. <u>Script for 911</u> <i>"Hello, this is a domestic violence offender alert on behalf of the insert agency name from SENTINEL regarding a protective order violation. We have just received a stationary exclusion zone alert from [offender's name]'s GPS equipment indicating that the offender may be in the vicinity of the following protected address [zone address]. Offender's last known location was [last known address] & was moving [direction & approximate speed of movement if available]."</i> If the victim was successfully contacted include the following: <i>"I spoke to the victim, [victim's name], & their stated location was [reported location]."</i> If the victim was not contacted, include the following: <i>"I tried calling the victim [victim's name] via cell phone & was unable to make contact."</i> <i>"The offender, [offender's name], is a [gender, race, height, weight, hair color, eye color, & date of birth], & may be driving a [vehicle description]."</i> The 911 dispatcher may ask the Monitoring Center for additional information. After all requested information has been provided tell the dispatcher your name & telephone number & ask, <i>"May I please have your name for our records?"</i>
EXCLUSION ZONE CLEARED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction: Call victim on all available numbers to inform them of clear, using script. If no answer, leave a voicemail. Input detailed notes then select Close.</i>	<u>Script for Stationary Exclusion Zone Clear for Victim or VM</u> <i>"Hello, this is SENTINEL calling for [victim's name]. We have received the clear for the stationary exclusion zone alert from [offender's name]'s GPS equipment indicating that the offender is no longer in the vicinity of [zone address]. Offender last known location was [last known address] & was moving [direction & approximate speed of movement if available]."</i>
EXCLUSION BUFFER ZONE ENTERED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims	<u>Script for Stationary Buffer Zone for Victim or VM</u> <i>"Hello, this is SENTINEL calling for [victim's</i>

	<i>Instruction: Call victim on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Close.</i>	<i>name]. We have just received a stationary buffer zone alert from [offender's name]'s GPS equipment indicating that the offender may be in the vicinity of [zone address]. Offender last known location was [last known address] & was moving [direction & approximate speed of movement if available]. I am providing this information so that you may implement your emergency procedures if you feel the need. We will continue to monitor the offender's location. If the offender enters the stationary exclusion zone, you will again be contacted."</i> <i>Ask for victim current location & whether to remain on the phone while implementing emergency procedures.</i>
EXCLUSION BUFFER ZONE CLEARED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction: Call victim on all available numbers to inform them of clear, using script. Input detailed notes then select Close.</i>	<u>Script for Stationary Buffer Zone Clear for Victim or VM</u> <i>"Hello, this is SENTINEL calling for [victim's name]. We have just received the clear for the stationary buffer zone alert from [offender's name]'s GPS equipment indicating that the offender is no longer in your vicinity of [zone address]."</i>
INCLUSION ZONE CLEARED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer	
INCLUSION ZONE ENTERED	<u>24/7</u> Step 1 - Role Based: Email Primary Officer	
INCLUSION BUFFER ZONE CLEARED		
FAILED TO ENTER	<u>24/7</u> Step 1 - Role Based: Email Primary Officer	
UNAPPROVED LEAVE	<u>24/7</u> Step 1 - Role Based: Email Primary Officer	
UNAPPROVED ENTER	<u>24/7</u> Step 1 - Role Based: Email Primary Officer	
UNAPPROVED INCLUSION ZONE CLEARED		
UNAPPROVED INCLUSION ZONE ENTERED		

UNSCHEDULED LEAVE (UNS LV)		
XMTR TAMPER - GPS	24/7 Step 1 - Role Based: Email Primary Officer Step 2 - Auto Email: TBD Step 3 - Contact Victims <i>Instruction:</i> Verify with dispatch that no service of install is currently being worked for the client in question. If dispatch has confirmed that the client is being serviced, input notes and CLOSE the alarm by selecting --Continue-- then navigate to the Pending Alarms list and select the --Stop Notifications-- button. If dispatch has confirmed the client is NOT being serviced, call victim on all available numbers using script. If no answer, leave a voicemail. Input detailed notes then select Continue. Step 4 - MC App <i>Instruction:</i> Call 911 for the city of the victim's current location only if they answered and provided their location and/or the last known location of the GPS device. If victim location is not known and/or does not answer, call 911 for the city of the offender's current location and also call 911 of the city where the victim lives only if victim did not answer or victim cannot provide their current location and/or does not have a GPS. Input detailed notes then select CONTINUE. Step 5 - Contact Victims <i>Instruction:</i> Check activity. If victim was already contacted, input notes then select CONTINUE. If unsuccessful in contacting victim the first time, make a second attempt on all available numbers using script. Input detailed notes then select CONTINUE. Step 6 - Role Based: Email 24/7 Contact (tamperofficevnp@sentineladvantage.com)	Script for Backplate/Strap Tamper for Victim or VM (911 Must be called at all times) <i>"Hello, this is SENTINEL calling for [victim's name]. Are you safe & can you freely speak, yes or no?"</i> If victim says no, immediately call 911 from a different line. If victim is free to speak ask for current location & continue: <i>"We have just received a tamper alert from [offender's name]'s GPS equipment indicating that the offender may have tried to damage or remove the GPS device. Offender last known location was [last known address] & was moving [direction and approximate speed of movement if available]. I am providing this information so that if you feel the need you may implement your emergency procedures, which may include your calling 911."</i> NOTE: Also, ask if victim would like you to remain on the phone while implementing emergency procedures. If victim is not safe/free to speak you should call 911 on a separate phone or have another operator call. Remain on the line & never put the victim on hold or mute when calling 911. Script for 911 (Call 911 of the city where the victim is located; If victim location is not known and/or no answer then call 911 of the offender's current location & city of the victim's home address) <i>"Hello, this is a domestic violence offender alert on behalf of the insert agency name from SENTINEL regarding a protective order violation. We have just received a tamper alert from [offender's name]'s GPS equipment indicating that the offender may have damaged or removed his/her tracking device. I spoke to the victim, [victim's name], who indicated that they were not safe & not free to speak. Victim location is [victim's last known location] & the offender may be nearby. The offender's last known location was [last known address & the time of the tamper] & was moving [direction & approximate speed of movement if available]. The offender, [offender's name], is a [gender, race, height, weight, hair color, eye color, & date of birth], & may be driving a [vehicle description]."</i>

		The 911 dispatcher may ask the Monitoring Center for additional information. After all requested information has been provided tell the dispatcher your name & telephone # & ask, <i>"May I please have your name for our records?"</i> NOTE: You may be asked for the information again, if call is forwarded (e.g. to local police dispatcher)
XMTR TAMPER RESET - GPS	<u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - Contact Victims <i>Instruction:</i> Call victim on all available numbers to inform them of clear. If no answer, leave a voicemail. Input detailed notes then select Close.	
BACKPLATE TAMPER	Same as Strap Tamper.	Same as Strap Tamper.
BACKPLATE TAMPER RESET	Same as Strap Tamper.	
NO GPS 1HR	**Auto Clear Event: No GPS - Clear** <u>24/7</u> Step 1 - Role Based: Email Primary Officer Step 2 - MC App <i>Instruction:</i> Call offender on all available numbers to troubleshoot. If alert is due to a low battery, use Low Battery script. If alert is NOT due to a low battery, advise offender to plug in device then run a current location during the call. If clear is received, input detailed notes then select CLOSE. If no answer, leave a voicemail using Low Battery script then input notes and select CONTINUE. If during troubleshooting the clear is NOT received after running 2 current locations, ask offender to step outside for 10 min. If extensive troubleshooting continues to be unsuccessful, input detailed notes then select CONTINUE. Step 3 - Contact Victims <i>Instruction:</i> Call victim on all available numbers using script. If no answer, leave a voicemail. If the victim is unable to speak or states they are unsafe, then proceed to call 911 using script. If the victim states they are safe, do NOT call 911. Input detailed notes. If OFFENDER did NOT answer previously when called for troubleshooting, then select CLOSE. If you were able to reach the offender to troubleshoot, then select CONTINUE. Step 4 - Auto Email: Primary Officer	<u>Script for Low Battery for offender</u> <i>"This is SENTINEL calling. You must charge your device for two continuous hours immediately. If you fail to charge your GPS device as instructed, your Family Relations Counselor & the local authorities will be notified."</i> <u>Script for No Communication and No Location for Victim or VM</u> <i>"Hello, this is SENTINEL calling for [victim's name]. Are you safe & can you freely speak, yes or no?"</i> If the victim says no, immediately call 911 from a different line. If the victim is free to speak ask for current location & continue: <i>"We have received a No Communication/No Location alert from [offender's name]'s GPS equipment which is no longer tracking. Their last known location was [last known address] & they were moving [direction & approximate speed of movement if available]. I am providing this information so that if you feel the need you may implement your emergency procedures, which may include your calling 911."</i> Also, ask if victim would like you to remain on the phone while implementing emergency procedures. If victim is not safe/free to speak & you know the victim location, you should call 911. If victim is not safe/free to speak you should call 911 on a separate phone or have

		another operator call. Remain on the line & never put the victim on hold or mute when calling 911. If the victim asks for more information, inform the victim that we will continue troubleshooting with the offender. If we made contact with the offender for a service please let the victim know & that we will call them once it is resolved. If the victim still fears for their safety offer to call 911 or inform the victim they can call 911. Also if the victim still needs more information direct the victim to contact Family Service office & provide the victim with the contact information. <u>Do not give information that is older than 12 hours,</u> any further information outside the current alert needs to be directed to the Family Counselor. <u>Script for 911</u> (Only if the victim is not safe/free to speak & you know the victim's location) "Hello, this is a domestic violence offender alert on behalf of the insert agency name from SENTINEL regarding a protective order violation. We have just received a No Communication/No Location alert from [offender's name]'s GPS equipment which is no longer tracking. I spoke to the victim, [victim's name], who indicated that they were not safe & not free to speak. Victim location is [victim's last known location if available] & the offender may be nearby. The offender's last known location was [last known address & the time of the alert] & they were moving [direction & approximate speed of movement if available]. The offender, [offender's name], is a [gender, race, height, weight, hair color, eye color, & date of birth], & may be driving a [vehicle description]." The 911 dispatcher may ask the Monitoring Center for additional information. After all requested information has been provided tell the dispatcher your name & telephone # & ask, "May I please have your name for our records?"
NO GPS - CLEAR	<u>24/7</u> Step 1 - Contact Victims <i>Instruction:</i> Check activity. If victim and/or 911 were NOT previously notified on a No GPS alert, then select CLOSE. If victim and/or 911 were previously notified on a No GPS alert, then contact victim and/or 911 to inform them of clear. Input detailed notes and select	<u>No Communication/No Location clears to victim and/or 911</u> "This is SENTINEL calling to inform you that the No Communication/Location alert for (Offender Name) has cleared."

	CONTINUE. Step 2 - Role Based: Email Primary Officer	
NO CELL 1HR	<u>**Auto Clear Event: No Cell - Clear**</u> Same as No GPS 1 Hr.	Same as No GPS 1 Hr.
NO CELL - CLEAR	<u>24/7</u> Step 1 - Contact Victims <i>Instruction:</i> Check activity. If victim and/or 911 were NOT previously notified on a No Cell alert, then select CLOSE. If victim and/or 911 were previously notified on a No Cell alert, then contact victim and/or 911 to inform them of clear. Input detailed notes and select CONTINUE. Step 2 - Role Based: Email Primary Officer	Same as No GPS Clear.

Service Level Agreement – Category 2: RF

SERVICE LEVEL AGREEMENTS

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements (“SLAs”).

PERFORMANCE OBJECTIVES

Sentinel has established standards that serve as minimum performance criteria throughout the company. These standards will not be enforced as contradictory to the orders of any customers but, rather, to ensure that Sentinel manages the offender monitoring process to the highest possible level of consistent professionalism possible. The Quality Management Team will routinely revise company standards as needed and publish these revisions through memos, emails, checklists and Standard Operating Procedure (SOP) changes. These company standards, regardless of the medium employed for communicating them, will be adhered to as the minimum standards for Sentinel and will be effective immediately as indicated.

Along with these Universal Standards a series of checklists and Key Performance Indicator Reports will be available to employees in all departments and/or at field offices for purposes of self-evaluating their compliance with standards both applicable to the company as well as their department/office. Where local differences may exist between the Universal Standards and the Participating Entity standards, the highest possible standard that does not conflict with the Participating Entity’s standards will be observed.

Global KPIs (key performance indicators) from Department Heads are collected to evaluate the performance and the effectiveness of the quality management system. Global KPIs captures performance metrics for the following Departments: Monitoring Center, Quality, Training, Human Resources, Production, and Technology. These Monthly reports will be made available to the Participating Entity upon request.

Sentinel collects data throughout our operation that allows us to effectively report on the significant metrics outlined in this section.

- 1) Our trained Equipment Service personnel record device RMA (return material authorization) evaluation results in Sentinel’s Home Inventory program. Daily Sentinel monitors devices return, along with the description of the malfunction and captures the root cause. These findings are reviewed monthly with senior management and corrective actions are implemented if device malfunction rates warrant. Monthly evaluation reports are available upon request to our customers.
- 2) Our Evaluation report captures return date, evaluation date, and repair completion date. This report demonstrates the responsiveness to issues and speed to resolution which Sentinel has implemented to resolve outstanding issues.
- 3) All devices returned are evaluated and tested to conform to Sentinel’s stringent FQC (final quality control) requirements to confirm that the unit is fully functional at the time of shipment. Moreover, all device maintenance is captured in Sentinel’s Home Inventory program to ensure device calibration and maintenance schedules are adhered to. Maintenance records are available to our customers upon request.
- 4) Local operating procedures are established at the agency level to ensure adherence to court-ordered schedules for installation and removal of Products and Services.
- 5) Sentinel works directly with the Participating Entity personnel to establish reporting protocols at the outset of the program. These protocols serve as the basis for monitoring response and

performance measurement. These protocols establish the timeliness of response and report submittal requirements required by the Participating Entity.

- 6) Sentinel will provide complete transparency and results of our internal reporting. At the Participating Entities request we will complete the mandatory or specific government evaluation forms documenting our performance.
- 7) Training department periodically distributes a customer survey upon completion of training to improve customer training experience. Training survey includes questions regarding training knowledge and training material. Results of those satisfaction surveys will be provided to the Participating Entities upon request.
- 8) The Director of QA periodically distributes an NPS Survey to all customers to improve overall service quality. The survey includes evaluation of all aspects of our operation including the Monitoring Center and Help Desk services. The results of these surveys provide guidance for our continual improvement efforts and results are available to our customer at any time.

SERVICE REQUESTS FROM PARTICIPATING ENTITY AND/OR PRODUCT USER

Sentinel responds to Product and Service request(s) from the User and Product User per the Participating Entity's Participating Addendum.

Sentinel is not responsible for Product User damage as defined as Product User misuse, neglect or abuse of an installed product and/or service, and Sentinel understands we retain the right to bill the Purchasing Entity and/or Product User at a fee schedule negotiated per the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

As an added benefit to Participating Entities, the Sentinel pricing proposed herein includes an annual volume of replacements for lost, damaged and/or stolen equipment equivalent to up to five percent (5%) of the units in active use on participants, at no additional cost. Lost, damaged and/or stolen replacement pricing proposed herein are for losses more than the included annual five percent (5%) replacements.

MAINTENANCE, SUPPORT AND SERVICING AGREEMENTS FOR PRODUCTS AND SERVICES

Sentinel understands and acknowledges that the Participating Entity may negotiate and incorporate into its Participating Addendum, product maintenance, support and/or servicing agreements for any products and/or services purchased outright or rented by the Participating Entity.

Sentinel understands and acknowledges that, unless otherwise determined by the Participating Entity, pricing is based on a flat rate monthly fee which at a minimum includes but is not limited to; Contractor time and materials, and preventative maintenance. We understand and acknowledge that the term of such an agreement cannot exceed the useful life of the product(s) and/or services rendered as determined by either the Product and/or Service Manufacturer and/or the Participating Entity.

MAINTENANCE, SUPPORT AND SERVICING TECHNICIANS, PREVENTATIVE MAINTENANCE AND REPAIR PARTS AND SERVICE LOGS

Sentinel Employs Service Technicians for all OEM equipment.

Sentinel is the OEM or authorized distributor and as such the Service Technicians are properly trained and certified according to Sentinel's ISO Certification.

PREVENTATIVE MAINTENANCE & REPAIR PARTS

Sentinel performs all preventative maintenance services at the Product Manufacturer's directed intervals, or as specified by a Participating Addendum.

Sentinel ensures all product components, spare parts, and ancillary equipment that is supplied under the Master Agreement, will conform to manufacturer specifications including for use interfacing with proposed information technology solution(s).

Sentinel is responsible for ensuring that any repair parts are operable and installed in accordance with manufacturer specifications.

Sentinel ensures repair parts are new.

SERVICE LOGS

Sentinel maintains a digital record in the Repairs portal housed in Home Inventory System. This Repairs portal allows for a full history of all preventative maintenance and repairs performed on each piece of Monitoring Equipment.

Upon request, Sentinel provides digital service log(s) and/or requested information to the Participating Entity within three (3) calendar days of request.

PRODUCT AND SERVICE DELIVERY SPECIFICATIONS

For urgent orders and orders that require Priority Shipping, a Shipping Quote will be provided to the Participating Entity.

Sentinel understands and will provide a shipping quote prior to order placement from the Participating Entity for urgent orders that require priority shipping.

Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, CA and Alpharetta, GA. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities.

All orders will ship within one (1) business day of receipt and will be delivered FOB unless otherwise directed by the Participating Entity.

As appropriate, Sentinel can ship product(s) overnight in emergency cases as deemed necessary by the Participating Entity and pursuant to the timeframes specified in the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

To minimize the emphasis on expedited shipments, Sentinel pricing proposed herein includes an on-site spare inventory of equipment equivalent to up to fifteen percent (15%) of the units in active use on participants, at no additional cost. Further, Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, California, and Alpharetta, Georgia. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities. Sentinel provides regular ground shipments to Participating Entities at no additional cost.

MONITORING SERVICES AND REQUIREMENTS FOR PRODUCTS AND SERVICES

Sentinel maintains monitoring center(s), within the United States. Sentinel's monitoring center(s) are equipped with redundant internet and telephone connectivity, as well as all other equipment required for

performance of all monitoring activities required pursuant to the proposed and awarded Products and Services under the Master Agreement.

Sentinel's datacenters are all located within the United States. All datacenters have uninterruptible power supplies and backup generators. The Primary facility in Los Angeles has backup internet service that can be used in the event of a major outage with the primary internet service. All critical components of Sentinel's Primary Information System are continuously replicated to our geographically redundant Secondary Information System in Dallas, Texas. Sentinel's Primary Information System is hosted on hardware maintained by Sentinel staff in a secure collocation facility in Los Angeles, California. The facility provides a full uninterruptible power supply (UPS), Generator, and redundant power circuit backups. Sentinel maintains separate AT&T and Sprint internet circuits in the Primary Information System for website and unit communication failover purposes. In the event of a disaster or failure, Sentinel can re-point websites and tracking unit communication to any provider or IP addresses to maintain the flow of traffic. Land Line traffic is provided by geo-redundant SIP trunks with Cox Communications with ability to failover to the Secondary Site automatically in the event of a failure.

Sentinel's Monitoring Center staff is decentralized and staffed across the United States so telephone impact due to a single location or entire geographic zone is minimized. Sentinel's primary National Monitoring Center is in our Norco, California, corporate facility and Sentinel's secondary Monitoring Center is in our Atlanta, Georgia, facility.

The cloud sections of Sentinel's application are deployed in reputed Oracle Government Cloud with primary services at Ashburn, Virginia and disaster recovery in Phoenix, Arizona. Both facilities have datacenter-grade hardware with redundant power supply and internet services.

The Sentinel monitoring center is available and staffed 24 hours a day, 7 days a week, 365 days a year through toll-free telephone and fax numbers to monitor Product User activity including activities in violation as defined by each respective Participating Entity's Participating Addendum. The monitoring operators and technicians are trained, experienced and capable of resolving most technical problems over the telephone or through remote diagnostics. In the unlikely event that problem solving requires a higher-level of involvement, Sentinel customer service is staffed by experienced technicians, each with diagnostic computer equipment to provide quick analysis and resolution of problems.

Databases are backed up offsite using Veeam to create and store 15-minute transaction logs, daily VM incremental snapshots, weekly synthetic full snapshots, and monthly active full backups.

Cloud databases are fully backed up weekly and incremental backup every three (3) hours. Additionally, a standby database at the disaster recovery location is continuously synched down to one (1) second.

Monthly, by the 5th business day of every month, the Director of Quality Assurance produces a System Availability and Performance report that captures the System Availability and performance of the Hosted Services during the calendar month. Report includes:

- 1) System uptime percentage.
- 2) Incident details.
- 3) Root cause(s) and corrective action (s) to prevent recurrence
- 4) Sentinel makes these reports available to Participating Entities upon request.

PRODUCT USER MONITORING AND ACTIVITY REPORTS

Sentinel allows unlimited access to an unlimited number of service requests by Participating Entities regarding Product User inquiries and/or service requests.

The proposed Sentinel monitoring platforms provides customizable methods and parameters of violation notification to the Users and shall accommodate changes and customization at the Participating Entity's request. The proposed Sentinel monitoring platforms provide methods for notification of Users and Product Users including immediate and next calendar day notifications via secure email, phone voice message, and cellular text message.

The proposed Sentinel monitoring platforms provides digital activity reports for all products and services deployed by the Participating Entity based on the required content specifications within the Participating Addendums.

Reports are available on the proposed Sentinel monitoring platforms via any web-enabled computer through the authorized user's login credentials (username and password). Reports are available on demand in standard format (Word, Excel, PDF), and Sentinel works with the Participating Entity to create customized reports.

Through the proposed Sentinel monitoring platforms, referring Users can enroll, terminate, modify, generate reports, add notes and otherwise perform Product User case activities through any internet-enabled device as well as by fax, email, and/or telephone.

Additionally, Sentinel's National Monitoring Center operators are available by fax, email, and/or telephone 24 hours a day, 7 days a week, 365 days a year to assist with enrollments, terminations, modifications, generating reports, adding notes, and otherwise assist with Product User case notes.

MONITORING SERVICE REQUIREMENTS

If Sentinel is authorized by a Participating Entity to invoice a Product User directly, the on-site Sentinel staff will establish in writing with Product User the fee schedule based on the policies and procedures established by the Participating Entity. Thereafter, for those program participants requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule established in writing with the Product User during their orientation.

Sentinel understands and will disclose information pertaining to how Product User data is collected and utilized by Sentinel or any subcontractor.

TRAINING REQUIREMENTS FOR USERS AND PRODUCT USERS

Customer training for Participating Entity authorized users is primarily coordinated by the Regional Account Manager (RAM) with Sentinel's Training Department. The Training Department will work together with the RAM to ensure each customer trainee has all the proper training documents (user guides, user manuals, PowerPoint presentations, reference guides, etc.). Training is provided via in person training, virtual training sessions, and Instructor Led Training sessions (ILTs). For Product Users, installation guides, installation training videos, and ILTs are available upon request.

Sentinel training sessions are tailored to the Participating Entity's Category of Need. The Training Department will work together with the RAM to determine the Participating Entity's Category of Need and tailor the Training Agenda to the Participating Entity's needs as documented on the Customer's Training Attendance Log, including but not limited to, Operation of the Product and/or Service including any web-based information system, Installation, deactivation, removal and operation of Products and Services, Product and Service return processes and Other as specified by the Participating Entity. Customers can utilize our user-friendly RMA Request Form for Product and Services Return processes.

Sentinel's Training Department provides training as needed by the Participating Entity and will complete training within ten (10) calendar days of the request unless otherwise specified by the Participating Addendum. Sentinel requests as much advance notice as possible for in person on-site training so that

travel arrangements can be made in advance.

Upon introduction of any new Product and Service feature, or whenever a user agency may need refresher training, the Sentinel Training Department will make available user guides, user manuals, PowerPoint presentations, reference guides, training videos, and provide Instruction Led Trainings (ILTs) virtual trainings upon request, at no additional charge to the Participating Entity.

Sentinel makes digital training materials readily available upon request and provides unlimited access to on-line resources at no charge to the Participating Entity.

Sentinel provides a 24/7/365 toll free phone number and an email address for technical support. Participating Entities can contact Sentinel 24/7/365 at 800-589-6003 opt 2 or email Monitoring_center@sentineladvantage.com for customer support and receive an immediate response 24 hours per day.

SAMPLE RF MONITORING NOTIFICATION PROTOCOL PROCEDURES

As part of on boarding with Participant Entities Sentinel works closely with the agency to set up Notification Protocol Procedures in our Monitoring Application. The following is a sample of our Radio Frequency (RF) monitoring notification protocol Form used for setting up Participating Entities Notification Protocol Procedures and flexibility to establish unique notification Protocol Procedures specific to the Participating Entities' needs and requirements.

ALARM	ALARM CLEARS	ALARM RESPONSE
HMU LOW BATTERY	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
XMTR LOW BATTERY	ENABLE CLEAR LINK	24/7 Step One - Auto Email Emails: Primary Officer
AC POWER DISCONNECT	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - McApp <i>Instruction:</i> Call participant on all available numbers and troubleshoot power disconnect. Insert detailed notes and Select CLOSE.
AC RESTORE	ENABLE CLEAR LINK	
TELEPHONE DISCONNECT	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
TELEPHONE RESTORE	ENABLE CLEAR LINK	
LEAVE	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
ENTER	ENABLE CLEAR LINK	
GUEST LEAVE	ENABLE CLEAR LINK	
GUEST ENTER	ENABLE CLEAR LINK	
FAILED TO LEAVE	ENABLE CLEAR LINK	

	ENABLE AUTO CLEAR EVENT	
FAILED TO ENTER	GRACE PERIOD ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
LATE TO ENTER	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
UNAPPROVED LEAVE	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
UNAPPROVED ENTER	ENABLE CLEAR LINK	
UNSCHEDULED LEAVE (UNS LV)	GRACE PERIOD ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 2HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 4HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 6HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 8HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 10HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 12HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 24HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
NO RETURN 24HR+	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
XMTR TAMPER	ENABLE CLEAR LINK	24/7

	ENABLE AUTO CLEAR EVENT	Step 1 - TEXT All Victims Step 2 - McApp <i>Instruction:</i> Call participant on all available numbers and instruct them to report the next business day with HMU for equipment inspection. Insert detailed notes, select Close.
XMTR TAMPER RESET	ENABLE CLEAR LINK	
XMTR TAMPER (HMU)	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step 1 - TEXT All Victims Step 2 - Auto Email Emails: OFFICER EMAIL: TBD Delay: 15 Minutes Step 3 - McApp Emails: TBD <i>Instruction:</i> Call PT using the following script, "Hello this is the Monitoring Center calling for (PT Name). You have been selected for a random equipment inspection and are to report to the Pretrial office next business day by 09:00." If no answer, leave VM. Specify if PT refuses to report to the office. Insert detailed notes with outcome of call. Select NOTIFY, then COMMENT, then CLOSE.
XMTR TAMPER RESET (HMU)	ENABLE CLEAR LINK	
HMU TAMPER	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - McApp <i>Instruction:</i> Call participant on all available numbers and get a statement. Insert detailed notes and Select CLOSE.
HMU TAMPER RESET	ENABLE CLEAR LINK	
HMU LTT	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU LTT 1HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU LTT 2 HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU LTT 3 HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU LTT 4HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU LTT 8HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR	

	EVENT	
HMU LTT 12 HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - McApp Instruction: Call participant on all available numbers and troubleshoot. Insert detailed notes and Select CLOSE.
HMU LTT 24HR	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - Auto Email and McApp Emails: OFFICER EMAIL: TBD Instruction: Call participant on all available numbers and instruct them to report for an equipment inspection. Advise PT to bring HMU and power cord. Insert detailed notes and Select CLOSE.
HMU LTT 24HR+	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - Auto Email and McApp Emails: OFFICER EMAIL: TBD Instruction: Call participant on all available numbers and instruct them to report for an equipment inspection. Advise PT to bring HMU and power cord. Insert detailed notes and Select CLOSE.
HMU SHUTDOWN	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	
HMU MOTION	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - McApp Instruction: Call participant on all available numbers to resolve. Insert detailed notes and Select CLOSE.
HMU MOTION WITH DISCONNECT	ENABLE CLEAR LINK ENABLE AUTO CLEAR EVENT	24/7 Step One - McApp Instruction: Call participant on all available numbers to resolve. Insert detailed notes and Select CLOSE.
NO CONNECTION	ENABLE CLEAR LINK	
NO DIAL TONE	ENABLE CLEAR LINK	

Service Level Agreement – Category 3: Alcohol Monitoring

SERVICE LEVEL AGREEMENTS

Sentinel understands and acknowledges that the Participating Entity may negotiate their own Service Level Agreements (“SLAs”).

PERFORMANCE OBJECTIVES

Sentinel has established standards that serve as minimum performance criteria throughout the company. These standards will not be enforced as contradictory to the orders of any customers but, rather, to ensure that Sentinel manages the offender monitoring process to the highest possible level of consistent professionalism possible. The Quality Management Team will routinely revise company standards as needed and publish these revisions through memos, emails, checklists and Standard Operating Procedure (SOP) changes. These company standards, regardless of the medium employed for communicating them, will be adhered to as the minimum standards for Sentinel and will be effective immediately as indicated.

Along with these Universal Standards a series of checklists and Key Performance Indicator Reports will be available to employees in all departments and/or at field offices for purposes of self-evaluating their compliance with standards both applicable to the company as well as their department/office. Where local differences may exist between the Universal Standards and the Participating Entity standards, the highest possible standard that does not conflict with the Participating Entity’s standards will be observed.

Global KPIs (key performance indicators) from Department Heads are collected to evaluate the performance and the effectiveness of the quality management system. Global KPIs captures performance metrics for the following Departments: Monitoring Center, Quality, Training, Human Resources, Production, and Technology. These Monthly reports will be made available to the Participating Entity upon request.

Sentinel collects data throughout our operation that allows us to effectively report on the significant metrics outlined in this section.

- 1) Our trained Equipment Service personnel record device return material authorization (RMA) evaluation results in Sentinel’s Home Inventory program. Daily Sentinel monitors devices return, along with the description of the malfunction and captures the root cause. These findings are reviewed monthly with senior management and corrective actions are implemented if device malfunction rates warrant. Monthly evaluation reports are available upon request to our customers.
- 2) Our Evaluation report captures return date, evaluation date, and repair completion date. This report demonstrates the responsiveness to issues and speed to resolution which Sentinel has implemented to resolve outstanding issues.
- 3) All devices returned are evaluated and tested to conform to Sentinel’s stringent FQC (final quality control) requirements to confirm that the unit is fully functional at the time of shipment. Moreover, all device maintenance is captured in Sentinel’s Home Inventory program to ensure device calibration and maintenance schedules are adhered to. Maintenance records are available to our customers upon request.
- 4) Local operating procedures are established at the agency level to ensure adherence to court-ordered schedules for installation and removal of Products and Services.
- 5) Sentinel works directly with the Participating Entity personnel to establish reporting protocols at the outset of the program. These protocols serve as the basis for monitoring response and

performance measurement. These protocols establish the timeliness of response and report submittal requirements required by the Participating Entity.

- 6) Sentinel will provide complete transparency and results of our internal reporting. At the Participating Entities request we will complete the mandatory or specific government evaluation forms documenting our performance.
- 7) Training department periodically distributes a customer survey upon completion of training to improve customer training experience. Training survey includes questions regarding training knowledge and training material. Results of those satisfaction surveys will be provided to the Participating Entities upon request.
- 8) The Director of Quality Assurance periodically distributes an NPS Survey to all customers to improve overall service quality. The survey includes evaluation of all aspects of our operation including the Monitoring Center and Help Desk services. The results of these surveys provide guidance for our continual improvement efforts and results are available to our customers at any time.

SERVICE REQUESTS FROM PARTICIPATING ENTITY AND/OR PRODUCT USER

Sentinel responds to Product and Service request(s) from the User and Product User per the Participating Entity's Participating Addendum.

Sentinel is not responsible for Product User damage as defined as Product User misuse, neglect or abuse of an installed Product and/or Service, and Sentinel understands we retain the right to bill the Purchasing Entity and/or Product User at a fee schedule negotiated per the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

As an added benefit to Participating Entities, the Sentinel pricing proposed herein includes an annual volume of replacements for lost, damaged and/or stolen equipment equivalent to up to five percent (5%) of the units in active use on participants, at no additional cost. Lost, damaged and/or stolen replacement pricing proposed herein are for losses more than the included annual five percent (5%) replacements.

MAINTENANCE, SUPPORT AND SERVICING AGREEMENTS FOR PRODUCTS AND SERVICES

Sentinel understands and acknowledges that the Participating Entity may negotiate and incorporate into its Participating Addendum, product maintenance, support and/or servicing agreements for any Products and/or Services purchased outright or rented by the Participating Entity.

Sentinel understands and acknowledges that, unless otherwise determined by the Participating Entity, pricing is based on a flat fee which at a minimum includes but is not limited to, contractor time and materials, and preventative maintenance. We understand and acknowledge that the term of such an agreement cannot exceed the useful life of the product(s) and/or services rendered as determined by either the Product and/or Service Manufacturer and/or the Participating Entity.

MAINTENANCE, SUPPORT AND SERVICING TECHNICIANS, PREVENTATIVE MAINTENANCE AND REPAIR PARTS AND SERVICE LOGS

Sentinel Employs Service Technicians for all OEM equipment.

Sentinel is the OEM or authorized distributor and as such the Service Technicians are properly trained and certified according to Sentinel's ISO Certification.

PREVENTATIVE MAINTENANCE & REPAIR PARTS

Sentinel performs all preventative maintenance services at the Product manufacturer's directed intervals, or as specified by a Participating Addendum.

Sentinel ensures all product components, spare parts, and ancillary equipment that is supplied under the Master Agreement, will conform to manufacturer specifications including for use interfacing with proposed information technology solution(s).

Sentinel is responsible for ensuring that any repair parts are operable and installed in accordance with manufacturer specifications.

Sentinel ensures repair parts are new.

SERVICE LOGS

Sentinel maintains a digital record in the Repairs portal housed in Home Inventory System. This Repairs portal allows for a full history of all preventative maintenance and repairs performed on each piece of Monitoring Equipment.

Upon request, Sentinel provides digital service log(s) and/or requested information to the Participating Entity within three (3) calendar days of request.

PRODUCT AND SERVICE DELIVERY SPECIFICATIONS

For urgent orders and orders that require Priority Shipping, a Shipping Quote will be provided to the Participating Entity.

Sentinel understands and will provide a shipping quote prior to order placement from the Participating Entity for urgent orders that require priority shipping.

Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, California, and Alpharetta, Georgia. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities.

All orders will ship within one (1) business day Of receipt and will be delivered FOB unless otherwise directed by the Participating Entity.

As appropriate, Sentinel can ship product(s) overnight in emergency cases as deemed necessary by the Participating Entity and pursuant to the timeframes specified in the Participating Entity's Participating Addendum.

—IMPORTANT SENTINEL ADVANTAGE—

To minimize the emphasis on expedited shipments, Sentinel pricing proposed herein includes an on-site spare inventory of equipment equivalent to up to fifteen percent (15%) of the units in active use on participants, at no additional cost. Further, Sentinel will support and ship to the Participating Entities from one of our two warehouses located in Anaheim, California, and Alpharetta, Georgia. By using the most geographically effective location for shipping we can deliver products more quickly at a lower cost to our Participating Entities. Sentinel provides regular ground shipments to Participating Entities at no additional cost.

MONITORING SERVICES AND REQUIREMENTS FOR PRODUCTS AND SERVICES

Sentinel maintains monitoring center(s), within the United States. Sentinel's monitoring center(s) are equipped with redundant internet and telephone connectivity, as well as all other equipment required for

performance of all monitoring activities required pursuant to the proposed and awarded Products and Services under the Master Agreement.

Sentinel's datacenters are all located within the United States. All datacenters have uninterruptible power supplies and backup generators. The Primary facility in Los Angeles has backup internet service that can be used in the event of a major outage with the primary internet service. All critical components of Sentinel's Primary Information System are continuously replicated to our geographically redundant Secondary Information System in Dallas, Texas. Sentinel's Primary Information System is hosted on hardware maintained by Sentinel staff in a secure collocation facility in Los Angeles, California. The facility provides a full uninterruptible power supply (UPS), Generator, and redundant power circuit backups. Sentinel maintains separate AT&T and Sprint internet circuits in the Primary Information System for website and unit communication failover purposes. In the event of a disaster or failure, Sentinel can re-point websites and tracking unit communication to any provider or IP addresses to maintain the flow of traffic. Land Line traffic is provided by geo-redundant SIP trunks with Cox Communications with ability to failover to the Secondary Site automatically in the event of a failure.

Sentinel's Monitoring Center staff is decentralized and staffed across the United States so telephone impact due to a single location or entire geographic zone is minimized. Sentinel's primary National Monitoring Center is in our Norco, California, corporate facility and Sentinel's secondary Monitoring Center is in our Atlanta, Georgia facility.

The cloud sections of Sentinel's application are deployed in reputed Oracle Government Cloud with primary services at Ashburn, Virginia and disaster recovery in Phoenix, Arizona. Both facilities have datacenter-grade hardware with redundant power supply and internet services.

The Sentinel monitoring center is available and staffed 24 hours a day, 7 days a week, 365 days a year through toll-free telephone and fax numbers to monitor Product User activity including activities in violation as defined by each respective Participating Entity's Participating Addendum. The monitoring operators and technicians are trained, experienced and capable of resolving most technical problems over the telephone or through remote diagnostics. In the unlikely event that problem solving requires a higher-level of involvement, Sentinel customer service is staffed by experienced technicians, each with diagnostic computer equipment to provide quick analysis and resolution of problems.

Databases are backed up offsite using Veeam to create and store 15-minute transaction logs, daily VM incremental snapshots, weekly synthetic full snapshots, and monthly active full backups.

Cloud databases are fully backed up weekly and incremental backup every three (3) hours. Additionally, a standby database at the disaster recovery location is continuously synched down to one (1) second.

Monthly, by the 5th business day of every month, the Director of Quality Assurance produces a System Availability and Performance report that captures the System Availability and performance of the Hosted Services during the calendar month. Report includes:

- + System uptime percentage.
- + Incident details.
- + Root cause(s) and corrective action (s) to prevent recurrence
- + Sentinel makes these reports available to Participating Entities upon request.

PRODUCT USER MONITORING AND ACTIVITY REPORTS

Sentinel allows unlimited access to an unlimited number of service requests by Participating Entities

regarding Product User inquiries and/or service requests.

The proposed Sentinel monitoring platforms provides customizable methods and parameters of violation notification to the Users and shall accommodate changes and customization at the Participating Entity's request. The proposed Sentinel monitoring platforms provide methods for notification of Users and Product Users including immediate and next calendar day notifications via secure email, phone voice message, and cellular text message.

The proposed Sentinel monitoring platforms provides digital activity reports for all Products and Services deployed by the Participating Entity based on the required content specifications within the Participating Addendums.

Reports are available on the proposed Sentinel monitoring platforms via any web-enabled computer through the authorized user's login credentials (username and password). Reports are available on demand in standard format (Word, Excel, PDF), and Sentinel works with the Participating Entity to create customized reports.

Through the proposed Sentinel monitoring platforms, referring Users can enroll, terminate, modify, generate reports, add notes and otherwise perform Product User case activities through any internet-enabled device as well as by fax, email, and/or telephone.

Additionally, Sentinel's National Monitoring Center operators are available by fax, email, and/or telephone 24 hours a day, 7 days a week, 365 days a year to assist with enrollments, terminations, modifications, generating reports, adding notes, and otherwise assist with Product User case notes.

MONITORING SERVICE REQUIREMENTS

If Sentinel is authorized by a Participating Entity to invoice a Product User directly, the on-site Sentinel staff will establish in writing with Product User the fee schedule, including but not limited to any late fees, based on the policies and procedures established by the Participating Entity. Thereafter, for those program participants requiring the collection of fees, funds are collected on a weekly or bi-weekly basis according to the established payment schedule established in writing with the Product User during their orientation.

Sentinel understands and will disclose information pertaining to how Product User data is collected and utilized by Sentinel or any subcontractor.

TRAINING REQUIREMENTS FOR USERS AND PRODUCT USERS

Customer training for Participating Entity authorized users is primarily coordinated by the Regional Account Manager (RAM) with Sentinel's Training Department. The Training Department will work together with the RAM to ensure each customer trainee has all the proper training documents (user guides, user manuals, PowerPoint presentations, reference guides, etc.). Training is provided via in person training, virtual training sessions, and Instructor Led Training sessions (ILTs). For Product Users, installation guides, installation training videos, and ILTs are available upon request.

Sentinel training sessions are tailored to the Participating Entity's Category of Need. The Training Department will work together with the RAM to determine the Participating Entity's Category of Need and tailor the Training Agenda to the Participating Entity's needs as documented on the Customer's Training Attendance Log, including but not limited to, Operation of the Product and/or Service including any web-based information system, Installation, deactivation, removal and operation of Products and Services, Product and Service return processes and Other as specified by the Participating Entity. Customers can utilize our user-friendly RMA Request Form for Product and Services Return processes.

Sentinel's Training Department provides training as needed by the Participating Entity and will complete training within ten (10) calendar days of the request unless otherwise specified by the Participating Addendum. Sentinel requests as much advance notice as possible for in person on-site training so that travel arrangements can be made in advance.

Upon introduction of any new Product and Service feature, or whenever a user agency may need refresher training the Sentinel Training Department will make available user guides, user manuals, PowerPoint presentations, reference guides, training videos, and provide Instruction Led Trainings (ILTs) virtual trainings upon request, at no additional charge to the Participating Entity.

Sentinel makes digital training materials readily available upon request and provides unlimited access to on-line resources at no charge to the Participating Entity.

Sentinel provides a 24/7/365 toll free phone number and an email address for technical support. Participating Entities can contact Sentinel 24/7/365 at 800-589-6003 opt 2 or email Monitoring_center@sentineladvantage.com for customer support and receive an immediate response 24 hours per day.

SAMPLE ALCOHOL MONITORING NOTIFICATION PROTOCOL PROCEDURES

As part of on boarding with Participant Entities Sentinel works closely with the agency to set up Notification Protocol Procedures in our Monitoring Application. The following is a sample of our Alcohol Monitoring Notification Protocol Form used for setting up Participating Entities Notification Protocol Procedures and the flexibility given to establish unique notification Protocol Procedures specific to the Participating Entities' needs and requirements.

REMOTE BREATH NOTIFICATION PROTOCOL SAMPLE

Remote Breath Alert Type	Agent/Dispatch Contact	Client Contact	# of Attempts	Leave Voicemail	Suspend Duration	2 nd Suspend Duration
Battery Critical Low	YES	YES				
Device Housing Breach	YES	NA				
Extended Missed Communication	YES	YES				
Failed Test	YES	NA				
Missed Test	YES	YES				
Scheduled Test Not Received	YES	YES				
AFI Pending Review	YES	NA				

REMOTE BREATH

The following Remote Breath alerts, during the days (xx) from the hours of xx to xxx.

- + Battery Critical Low
- + Device Housing Breach
- + Extended Missed Communication
- + Failed Test
- + Missed Test
- + Scheduled Test Not Received
- + AFI Pending Review

1. Battery Critical Low

- a. The Monitoring Center will call the Client using the Client's phone number that Customer entered in SCRAM Optix.
 - If no answer, the Monitoring Center will leave a message, suspend the alert for X minutes, and attempt X more times; suspending the alert for X minutes each time.
 - If the phone is answered, the Monitoring Center will direct the Client to plug in the Remote Breath device until charged.
- b. If after X attempts there has been no response, the Monitoring Center will contact Customer's main phone number to escalate the alert.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. Please charge the Remote Breath device using the charger supplied by your Officer. ***Suspend alert for X minutes. If alert regenerates, contact Client again.***

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. After X attempts, we have been unsuccessful in reaching the Client or resolving the issue. Please contact the Client to resolve.

2. Device Housing Breach

- a. The Monitoring Center will call the Officer using Customer's main phone number.
 - The Monitoring Center will advise the Officer to have the Client report to the office as soon as possible.
- b. If the Monitoring Center cannot reach the Officer, a message will be left.

Script:

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. The alert received indicates that the Client has tampered with the Remote Breath device in a way that is prohibited. Please inspect the device for damage and tampering as soon as possible.

3. Extended Missed Communication

- a. The Monitoring Center will call the Client using the Client's phone number that Customer entered in SCRAM Optix.
 - If no answer, the Monitoring Center will leave a message, suspend the alert for X minutes, and attempt X more time; suspending the alert for X minutes each time.
 - If the phone is answered, the Monitoring Center will direct the Client to turn on the Remote Breath device to restore communications.
- b. If communications are not restored, the Monitoring Center will further troubleshoot, up to and including advising the Client to contact their Officer for equipment replacement.
- c. If after three attempts there has been no response, the Monitoring Center will contact Customer's main phone number to escalate the alert.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. Please turn on the Remote Breath device while I determine if communications can be restored. ***If communications are not restored, instruct Client again. *** Please, plug the Remote Breath device into the charger provided. ***If communications are not restored, instruct Client again.***Please contact your Officer to schedule a device Remote Breath replacement.

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. After X attempts, we have been unsuccessful in restoring communications. Please contact the Client to schedule a Remote Breath device replacement.

4. Failed Test

- a. The Monitoring Center will call the Officer using Customer's main phone number.
 - After making the initial call to the Officer, the Monitoring Center will begin sending on-demand breath tests every 20 minutes until the Client's breath test results are zero.
- b. Upon return to zero, the Monitoring Center will enter a note in the Client's record in SCRAM Optix.
- c. If the Client does not take the additional breath tests that are sent to the Remote Breath device, follow the Missed Test protocol.

Script:

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. We will be sending on-demand breath tests every 20 minutes until the Client's breath test results return to zero.

5. Missed Test

- a. The Monitoring Center will call the Client to notify that he/she has missed a scheduled breath test. This call will be made using the Client's phone number that Customer entered in SCRAM Optix.
- b. The Monitoring Center will begin sending on-demand breath tests and placing additional calls to the Client until breath test results are received. The alert will be suspended for a maximum of X/X minutes apart.
- c. Upon receipt of the breath test results, the Monitoring Center will enter a note in the Client's record in SCRAM Optix.

- d. If the Client does not respond, a call will be made to the Officer after two hours to notify that the Client has missed repeated breath tests.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. This call is to notify you that you have missed a scheduled Remote Breath Test. Please turn on the Remote Breath device and provide a breath test at this time.

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. The Client has missed a scheduled breath test and has been unresponsive in providing an on-demand breath test.

6. Scheduled Test Not Received

- a. The Monitoring Center will call the Client to notify that we have not received their scheduled breath test results. This call will be made using the Client's phone number that Customer entered in SCRAM Optix.
 - If no answer, the alert will be suspended for X minutes and the Monitoring Center will attempt a second call.
 - If the phone is answered, the Monitoring Center will troubleshoot the issue by asking the Client to turn on the Remote Breath device to identify the current cell coverage in the Client's location and/or the current battery voltage of the Remote Breath device.
 - The Monitoring Center will advise the Client to move to a better cellular coverage area as soon as possible or charge the Remote Breath device.
- b. If contact has not been made and if test results are not received, the Monitoring Center will call the Officer to report that results have still not been received.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. This call is to notify you that we have not received the results of your scheduled breath test. Please turn on the Remote Breath device and report the cellular coverage bars as seen on the device. Also report the battery voltage level on the Remote Breath device. Please relocate to an area that will increase the cellular coverage (by a window or outside) and/or plug in the Remote Breath device using the charger provided by your Officer.

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. We have not received the Client's breath test results. 1) We have been unable to reach the Client so please schedule an appointment with him/her, or 2) we have troubleshooted the Remote Breath device and need the Client to report to your office for advanced troubleshooting and/or device replacement.

7. AFI Pending Review

- a. The Monitoring Center will call the Officer using Customer's main phone number.
 - 1) The Monitoring Center will advise the Officer to review the alert in SCRAM Optix to determine if the Client attempted to circumvent the AFI technology or if the photographs can be matched.

Script:

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. Please review the AFI Pending Review alert on the Client's RB Results page to determine if the Client attempted to circumvent the technology or if the photographs can be matched.

CONTINUOUS ALCOHOL MONITORING (CAM) ALERTS

CAM Alert Type	Agent/Dispatch Contact	Client Contact	# of Attempts	Leave Voicemail	Suspend Duration	2 nd Suspend Duration
Critical Communication						
Replace Battery/Faceplate						
Low Battery						
Strap Replacement						
Annual Maintenance						

SCRAM CAM (CONTINUOUS ALCOHOL MONITOR)

The AMS Monitoring Center will respond to the following SCRAM CAM alerts during the days (xx) from the hours of xx to xxx.

- + Critical Communications
- + Replace Battery/Faceplate
- + Low Battery
- + Strap Replacement
- + Annual Maintenance

The Monitoring Center will follow up on these non-critical SCRAM CAM alerts on a daily basis.

1. Critical Communications

- a. The Monitoring Center will call the Client using the Client's phone number that Customer entered in SCRAM Optix.
 - If the phone is answered, the Monitoring Center will troubleshoot the communications issue. If communications are restored, AMS will enter a note in the Client's record and resolve the alert.
 - If no answer, the Monitoring Center will leave a message to upload the bracelet data using the selected communications method (Ethernet, Direct Connect or Base Station).

- If Direct Connect is being used as the method of communications, the Client will be instructed to contact their Officer for an immediate upload.
- b. If communications are not restored after X days, the Monitoring Center will call the Officer using Customer's main phone number and request that a physical inspection be performed on the SCRAM equipment.
 - Once the alert has been escalated to the Officer, the Monitoring Center will not place any further calls to the Client for that alert.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. This call is to notify you that we have not received data from the SCRAM CAM Bracelet at the scheduled upload time.

Based on the communications method being used, troubleshooting steps will commence
your bracelet communications have/have not been restored. Please contact your Officer to schedule a SCRAM equipment check.

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received a [Event Name] alert on [Client Name] at [Event Time and Time Zone]. We have notified the Client for X days that the assigned SCRAM CAM Bracelet is in a critical communications state and communications have not been restored. Please schedule a SCRAM equipment check and contact AMS Customer Services if advanced troubleshooting or RMA is required.

2. Maintenance Alerts- Battery/Faceplate, Low Battery, Strap Replacement, Annual Maintenance

- a. The Monitoring Center will call the Client using the Client's phone number that Customer entered in SCRAM Optix.
 - If no answer, the Monitoring Center will leave a message to contact their Officer to have maintenance performed.
 - If the phone is answered, the Monitoring Center will advise the Client to contact their Officer to schedule a bracelet maintenance appointment.
- b. If Client contact is not made for X days, the alert will be escalated to the Officer using Customer's main phone number and request that a physical inspection be performed on the SCRAM CAM Bracelet.
 - Once contact has been made with the Client or the alert has been escalated to Customer, the Monitoring Center will not place any further calls to the Client for that alert.

Script:

Calls to Client: This is the Monitoring Center. This call is being recorded. This call is to notify you that we have received a SCRAM CAM Maintenance alert. Please contact your Officer to schedule a SCRAM equipment maintenance appointment.

Call to Officer: This is the Monitoring Center. This call is being recorded. We have received an [Event Name] alert on [Client Name] at [Event Time and Time Zone]. We have notified the Client for two days that the SCRAM CAM Bracelet requires maintenance. Please schedule a SCRAM equipment maintenance appointment.

The OM500 offered by Sentinel is a sleek, one-piece GPS tracking device that employs GPS, WiFi, and Cellular location tracking technologies to effectively monitor a participant's movement throughout the community.

The device allows agency personnel to communicate with participants through the use of customized audio messaging, vibrations, and tones. The OM500 utilizes quick charge technology and offers industry leading battery performance.



ESSENTIAL FEATURES

- Extended battery life that exceeds five plus (5+) days on a single charge
- Participant communications via tone, vibration, and voice
- Reusable, fiber-optic strap and Optional Cut Resistant strap
- Tamper detection by fiber-optic strap and backplate removal
- Tracks indoors and GPS-impaired environments for greater accuracy
- Participant acknowledgement sensor
- Cellular, satellite, and Wi-Fi signals for precision tracking
- Verizon and AT&T LTE Networks
- Audio Siren 90+ decibel
- Rapid, rotating magnetic charger
- Waterproof, dishwasher safe, and exceeds IP68 standards
- One-piece design, tool-free installation



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

The OM500 Beacon, offered by Sentinel, is a sleek in-home device that provides accurate location data in challenging environments where GPS signals are limited or unavailable. Paired with the OM500, the Beacon uses a secure Wi-Fi connection to precisely verify presence or absence of the participant at a specific location.

The OM500 Beacon is particularly effective in situations where participants may be restricted to a certain apartment within a multi-level facility. The Beacon is able to assist in reporting the vertical and horizontal movement of the participant should they leave their assigned residence.



OM500 Beacon Benefits

- Reduces location failure alerts in challenging environments
- Immediately reports tampering when the device is opened, moved, or power is disconnected
- 20+ hour battery backup
- Simple installation completed in under 3 minutes
- Secure Wi-Fi connection minimizes zone size and behaves like curfew monitoring device
- OM500 reinitiates GPS upon leaving the range of the Beacon

Specifications

Location Technology	Wi-Fi
Physical	2.0" (h) x 6.5" (w) x 4.0" (d)
Weight	9.1 oz
Power Source	120 Volt
Battery Backup	20+ hrs
Tamper Features	Case open Power disconnect Device movement
Device Compabability	OM500 Series



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

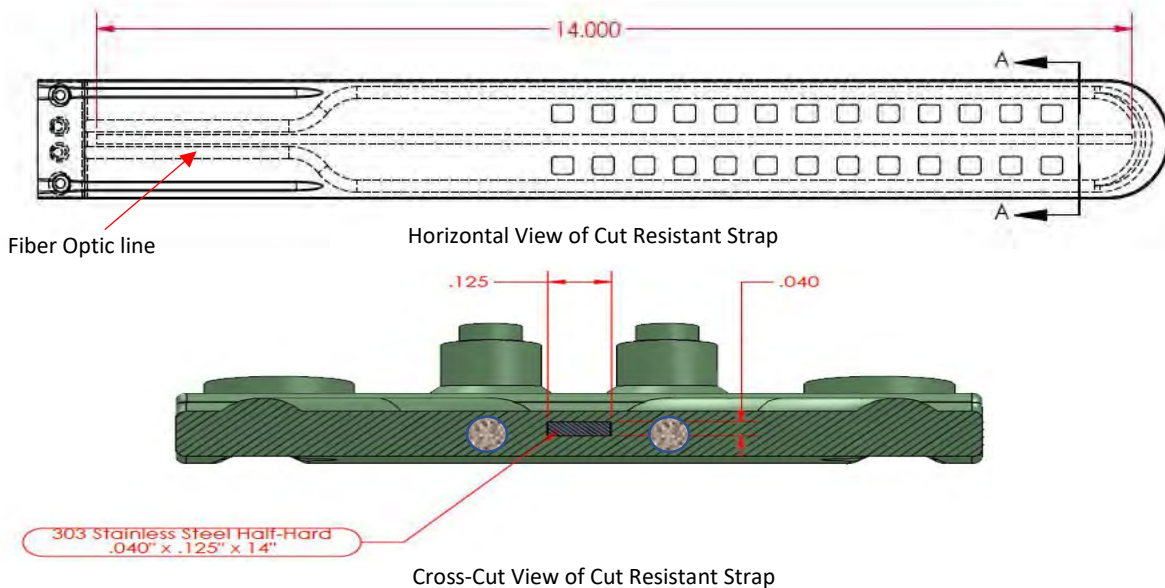
Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM



OM Series Cut Resistant Strap

Sentinel now offers a cut-resistant strap that can be used on any OM series offender monitoring solution. Sentinel added a thin heat-treated hardened stainless-steel strip to the existing industry-leading strap design for customers seeking a more secure strap. The hardened heat-treated stainless-steel strip is highly cut-resistant, providing additional layers of security to the existing tamper features of our time-tested reusable strap. The cut-resistant strap is made of thermoplastic polyurethane, which is hypoallergenic.



Sentinel does not recommend the use of cut-resistant straps except in certain controlled environments. The NIJ Offender Monitoring Standard 1004.00 requires that offender monitoring straps be cut with medical sheers in one minute or less, and the Sentinel cut-resistant strap does not meet this voluntary standard. Please contact your Account Manager for additional information about the Sentinel cut-resistant strap.

Advocate



Victim Notification and Tracking Application

Convenient, Discreet and Confidential

Combining a Victim's smartphone with the advanced tracking capabilities of Sentinel's OM500 GPS device, Advocate allows law enforcement and corrections agencies to track and compare location data of participants and Victims of domestic violence simultaneously through Sentinel's proprietary DNA monitoring system.

Available for iPhone and Android devices, Advocate discreetly tracks the Victim's smartphone and updates SentinelDNA with location data to create a Mobile Exclusion Zone. This Mobile Exclusion Zone repositions within SentinelDNA as the Victim's smartphone moves throughout the community. Should the participant approach within a preset distance of the Victim's smartphone, notification is sent to the Victim and law enforcement authorities.



ESSENTIAL FEATURES

Sentinel's Advocate App combines the services of our industry-leading 24/7/365 National Monitoring Center with proven GPS tracking technology to deliver:

- Near real-time Victim and participant geolocation comparison
- Convenient text, email, or push notifications without the need for a secondary device
- Configurable Exclusion Zone sizing for maximum program effectiveness
- 90+ decibel Siren for Alert Notification triggered on participant's GPS device
- Specially trained Sentinel operators providing 24-hour a day location monitoring and poised, reliable information to the Victim and law enforcement should an offender breach an exclusion zone
- Advanced notification with the use of customizable Buffer Zones
- Emergency contact numbers and one touch dialing for 911



At the Core of What We Do.

SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

Specifications

Width | 1.9 in



Height | 2.1 in



Weight | 3.7 oz

The ShadoWatch isn't just a tracking device; it's a fusion of cutting-edge security and ease of use. With its robust, one-piece design and advanced locating technologies, it sets the new standard for reliability and convenience in monitoring solutions.

PERFORMANCE DATA

GPS, Wi-Fi, & LBS
Tamper-Proof
Messaging
56 GPS Channels
IP68 Water-Proof
Onboard Memory
Cordless Charger
Bluetooth Technology and Heart Rate Sensor
Offender Vibration Alerts: Low battery, zone violation, etc.
Display size 1.3 in and TFTColorScreen
Two-Way Voice (optional)
Operating Temp: From -10°C:≥60%



Cordless | Power Cell

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P| 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

POWER CELL SPECIFICATIONS

- Input Voltage of the Whole Product= 5VDC
- **Mobile Charger:** Direct Magnetic Connection
- **Wired Charging:** Direct Magnetic Connection

POWER CELL CONSUMPTION



SUPPORTED ALARMS

- Device Communication Timeout
- Device Communication Timeout Escalated
- Failed to Charge
- Band Tamper
- Within Exclusion Zone
- Outside Inclusion Zone
- Lack of Motion
- Proximity Tamper
- Battery Critical
- No Location
- No Location Escalated



RF Patrol is among the most reliable and complete radio frequency (RF) home monitoring systems on the market. Its simple and durable design makes it the product of choice for agencies across the country.

The system is comprised of an ankle-worn transceiver and a stationary home monitoring unit (HMU). The HMU and transceiver continuously communicate with each other via RF signal. The HMU monitors any change in transceiver status and reports immediately to Sentinel's Monitoring Center via a cellular network to ensure timely notification to supervising officers.

The HMU can monitor up to 50 transceivers simultaneously making it ideal for halfway houses and group housing.



Transceiver



Home Monitoring Unit

ESSENTIAL FEATURES

Transceiver (ankle bracelet)

- Small, lightweight, durable
- Tamper resistant, fiber-optic strap
- Extended battery life
- Hypoallergenic material
- Waterproof up to 10 meters
- Low battery and tamper alarms

Home Monitoring Unit

- Easy to read front panel LCD
- Displays text messages from supervising officer
- Rechargeable backup battery, up to 48+ hours
- Adjustable range settings
- Cellular communication
- Tracks all entry and exits of participant
- Nonvolatile memory records more than 1,000 events



At the Core of What We Do.

SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

TRANSDERMAL ALCOHOL MONITORING

SCRAM CAM is the only scientifically proven and court-validated continuous transdermal alcohol monitoring device available. Technologies such as SCRAM CAM have taken center stage as a way to greatly enhance participant supervision and accountability at a fraction of the cost of incarceration.

SCRAM CAM provides flexible options for the type and intensity of supervision while enabling participants to maintain a job and meet family obligations. SCRAM CAM is the only continuous alcohol monitoring product that does not require a secondary test to confirm a drinking event by a participant.



Bracelet



Base Station

ESSENTIAL FEATURES

- Testing gaps are eliminated as participant cannot miss a test
- Automatically tests for the presence of alcohol every 30 minutes, 24 hours a day
- Used by 100,000+ offenders across the US
- Works well in conjunction with treatment to enforce compliance and better identify when intervention may be needed
- Automatically transmits participant data when in range of in-home base station
- Multiple sensors offer best-in-class tamper detection, placement of obstructions, and attempts to remove the device
- Flexible monitoring levels for multiple needs
- RF base station communicates with monitoring center via landline, cellular, or Ethernet
- Optional RF in-home monitoring station



At the Core of What We Do.

SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

Remote Breath Pro



The Most Versatile and Compact Breathalyzer
A SCRAM Device



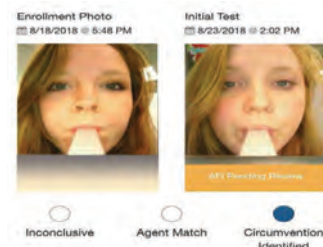
**Portable and durable alcohol testing
built for community corrections.**

SCRAM Remote Breath® Pro provides portable breath alcohol monitoring to ensure clients comply with court orders. The easy-to-use device is ideal for low-risk clients or those who have earned less intensive testing and monitoring.



Enhanced Facial Guidance and Authentication Software

- Provides visual cues ensuring face is aligned during client testing
- Increases client compliance by reducing the need for multiple tests
- Decreases officer photo manual matching 90-95%



Additional key features:

- GPS location with taken and missed tests
- Immediate notification of BrAC and client verification results
- Configurable scheduled and random testing schedules and testing grace periods
- Stores up to 40,000 test results when not in cell service and forwards upon return
- Optional testing reminders via text message

Portable and Discreet

This small and durable device adapts to clients' everyday life - enabling them to take tests anytime, anywhere. Includes a fitted carrying case and both standard wall outlet and USB charging ability.



With ShadowBriety, enrollees are checked regularly, randomly, or in the moment, for breath alcohol levels. Through facial recognition and Bluetooth technology, results are immediate, accurate, and specific to the enrollee.

HIGHLIGHTS INCLUDE:

- Random Sobriety Check
- Biometric Verification



SPECIFICATIONS	
Random or Scheduled Notifications	✓
Obtain Enrollee Location	✓
Anti-Spoofing Technology Built-In	✓
Facial Recognition Obtained	✓
Results Documented within the ShawodtrackONE Platform	✓
Bluetooth Connection	✓
Frequency Determined by Officer	✓
Caseload Management Integration	✓

SENTINEL'S 24/7/365 NATIONAL MONITORING CENTER PROVIDES THE SUPPORT YOU NEED

Sentinel's National Monitoring Center provides enhanced alert monitoring and officer support 24 hours a day, seven days a week, 365 days a year. The highly trained monitoring center personnel oversee a digital dashboard of mission critical information. These dedicated professionals ensure that automated and live-notification alerts are delivered smoothly to participants and supervising agencies.

Based on contracted specifications, any violation is quickly identified, confirmed, and possible cause verified. This information is passed along to the supervising officer and agency electronically and / or verbally. Monitoring Center personnel assist agencies in the completion of participant enrollments, the creation or editing of curfew schedules, the creation and management of GPS inclusion or exclusion zones, and also assist with alcohol testing. Monitoring Center personnel provide these support services:

- Assist users with all aspects of electronic monitoring and monitor alerts and violations 24 hours a day in real-time
- Provide around-the-clock diagnostic assistance and equipment and software troubleshooting support
- Deliver phone, email, SMS/text and fax updates 24/7/365.

Live Help Desk

Prior to a program's launch, Sentinel's Help Desk establishes all contract implementation procedures as required by the agency. Once established, help desk personnel are available to provide specialized technical support and advanced troubleshooting during peak business hours.



Help desk personnel provide written documentation and analysis of participant activity. This has been found to be an incredibly valuable service by supervising agencies and legal teams for internal purposes.

- Best-in-class electronic monitoring support services
- Advanced troubleshooting and high-level technical support
- Expert analysis documentation of electronic monitoring activity
- Report creation and analysis
- Creates and maintains custom agency profiles and notification procedures based on customer requirements
- Assists users with logins, passwords, enrollments, and alert processing information
- Inventory management: Orders and returns processing, inventory allocation, and the replacement of equipment
- Available by phone, email and fax Monday through Friday from 6:00 a.m. to 5:00 p.m. (Pacific)



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

SentinelDNA™ is the offender management platform that enables corrections agencies to monitor all of their program activities from any device. Users create customized dashboards for activity tracking, robust case management, inventory management, and advanced analytics.

Supervising officers can manage every aspect of a participant's case through a single screen. GPS tracking, electronic monitoring, remote alcohol testing, community based programs, and full service offender management are all accessible at the click of a button to handle even the largest caseloads.

Advanced Data Analytics allow you to take offender management to the next level. Make better, more well informed decisions with SentinelDNA.



Name	ID	Type	Equipment	Compliance	Battery
Doe, Jane	ID000422	GPS3			97%
Doe, John	ID000423	RF			
Doe, Jane	ID000425	RF/GPS3			92%
Doe, John	ID000199	BART			
Doe, Jane	ID000424	GPS3			92%

Supervising Officer Dashboard

ESSENTIAL FEATURES

- Customized Dashboards to meet unique programmatic needs
- Near real-time access to view and access participant activity in just a few keystrokes.
- Case management module provides access to features such as Court-Ordered Requirements, Financial Obligations, Drug Testing Requirements, and Counseling/Community Involvement Projects
- Comprehensive Inventory Management Module enables officers to track all program equipment
- Extensive Report Library allows officers to review participant/caseload activity, track equipment by device or participant, review participant payment history, create non-compliance reports, and audit user access to participant data
- Advanced Data Analytics allow officers to quickly identify known locations frequented by participants, record travel patterns, and recognize deviations from normal scheduled activities
- Event Detection provides participant proximity data to known crime scene locations



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

Designed to streamline feature sets that are available through our Sentinel DNA website, DNA Mobile improves the mobile access experience of our customers. Created using valuable input from a panel of supervising officers who routinely work away from their field office, DNA Mobile facilitates remote supervision like never before and will quickly become a valuable tool in participant supervision. DNA Mobile App, free to our customers, utilizes TLS 1.2, AES-256 encryption to ensure all customer and participant data is secure.



ESSENTIAL FEATURES

- Easily send commands to the GPS device
- View, respond, and clear alerts directly from DNA Mobile
- Quickly and easily send a text message to the participant's cellular based home monitoring unit
- Verify and document field contacts with participants while using DNA Mobile to record the date, time, location, and notes for each contact
- Quickly update a participant's curfew schedule
- Update client pictures directly through DNA Mobile
- Modify Participant name, Device ID, Case information, Home address, etc
- View GPS Tracking history, Current Location, and Zones via DNA Mobile
- Initiate Pursuit mode to activate faster GPS acquisition and reporting
- Get turn-by-turn directions from officer's location to the last known location of the participant or selected address
- Schedule and Review alcohol test results client picture, and GPS location directly from DNA Mobile
- Easily identify inventory availability and status



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

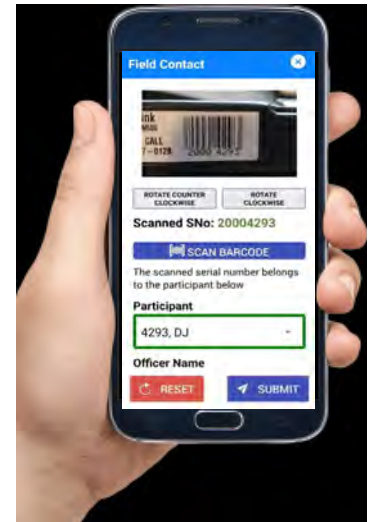
FIELD VERIFICATION MODULE

Complete and accurate record of participant contact

The Field Verification module for SentinelDNA allows field officers to efficiently verify and document interactions with program participants anytime and anywhere.

Using the SentinelDNA Mobile App, the officer scans the participant's GPS device to capture all pertinent information. The identity of the participant and officer are linked to the contact and the data is transmitted to SentinelDNA to become part of the permanent case file. Benefits include:

- **Simplicity:** Field officers quickly capture and document all pertinent information during field contact with a participant using their smartphone.
- **Convenience:** The participant's SentinelDNA record is automatically updated without after-the-fact manual entry of information.
- **Accountability:** Supervisors can ensure field contact with participants is documented and performed according to agency standards.



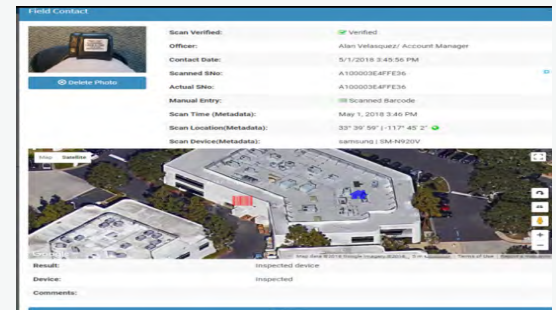
Verify field contact with participants using an iPhone or Android.

CAPTURES ESSENTIAL DATA

Field officers simply scan the participant's GPS device and all pertinent information is recorded, ad hoc notes can be added and data is electronically transmitted to SentinelDNA.

- **Who:** identity of program participant
- **Where:** location of the contact
- **When:** date and time contact took place
- **Field notes:** ad hoc notes and comments by officer
- **Agency-specific data:** user definable information
- **Part of the permanent record:** verified field contact with the participant becomes part of their historical record in SentinelDNA

FIELD VERIFICATION DATA ATTACHED TO CASE FILE



The Field Verification module for SentinelDNA provides proof of the date, time, and location of participant contact.



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

EQUIPMENT RETRIEVAL DASHBOARD

The SentinelDNA Equipment Retrieval Dashboard extends the value and effectiveness of inventory management. This easy-to-use tool tracks equipment that has yet to be retrieved when removing participants from your program.

The Equipment Retrieval Dashboard captures the participant's address, contact information, and equipment retrieval attempts so officers and supervisors can easily review equipment recovery efforts and reduce device loss. With easy to read reports outlining the status of each unreturned device, agencies are quickly able to identify lost devices reduce costs associated with lost equipment.

Reduce lost equipment by easily logging attempts to contact participant to retrieve devices.

Name	ID	Phone Number	Address	Equipment	Retrieval Date	Retrieval For	Officer / Case Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager
Participant: 0000000000	0000000000	0000 0000 0000	000 Technology Dr, Irvine, CA 92618	Smart (00111111)	00/00/0000	Other	Allen Rodriguez / Account Manager

Standardize retrieval efforts with customizable phases. For example: Phase 1: Call participant within the next 24 hours; Phase 2: Mail retrieval letter; Phase 3: Schedule drive by.

ESSENTIAL FEATURES

- Configurable retrieval phases define and standardize participant contacts and touch points
- Begin retrieval efforts quickly by automatically listing unreturned equipment at the time of participant removal from program
- Automatically flag equipment not recovered within 30 days
- Quickly view real time information about unreturned equipment, recovery efforts, officer assignment and the date of each recovery attempt
- Easy and fast look up of specific participant or device via the search box
- Automatically removes equipment that has been re-assigned to another participant, returned to Sentinel via RMA or identified as lost.



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring \$ Remote Alcohol Testing \$ Substance Abuse Screening
Domestic Violence Monitoring \$ Cognitive Skills Training \$ Full-Service Offender Management.

Call today to request a free demo or customized solution.

P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

© Copyright 2020 Sentinel Offender Services. All Rights Reserved.

EVENT DETECTION (CRIME SCENE CORRELATION)

SentinelDNA's Event Detection, also known as Crime Scene Correlation, allows agency personnel to determine if a participant was near a specific location during a specified time frame.

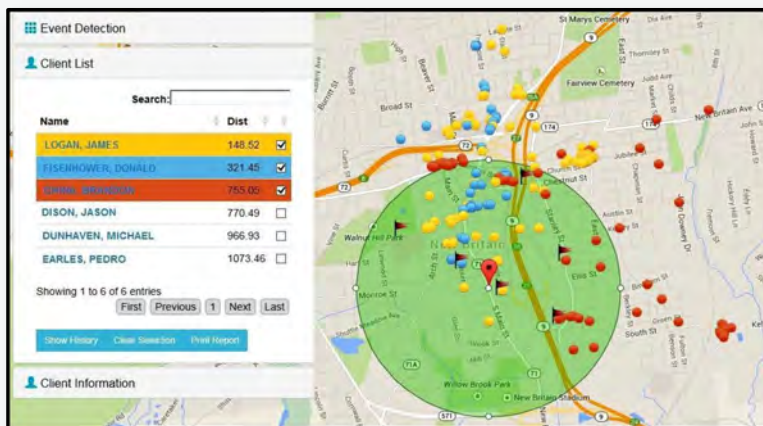
To access Event Detection, select "Event Detection" from the Reports menu in DNA.

Users will be directed to the Event Detection report interface on DNA Maps. Note: This is only available for participants on GPS monitoring.



A green circle will show the search area based on the criteria entered. The report will scan all activity during the selected time frame for any points showing within this circle. The results will show any participants within the zone around the address. To adjust the size of the search radius, click and drag one of the small white dots around the circle.

VIEWING MULTIPLE PARTICIPANT'S LOCATION HISTORY



Users may view the location history of up to three participants at a time within the event detection map for the time frame selected. To view the location history of participants for the time frame selected:

1. Select up to three participants from the Client List
2. Select "Show History"

Each participant's tracks will be displayed on the map in a different color. Hovering over a point on the map will display the participant's name and the date/time of the point.

The participant's name will be highlighted in the Client List with the corresponding color.



At the Core of What We Do.

SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

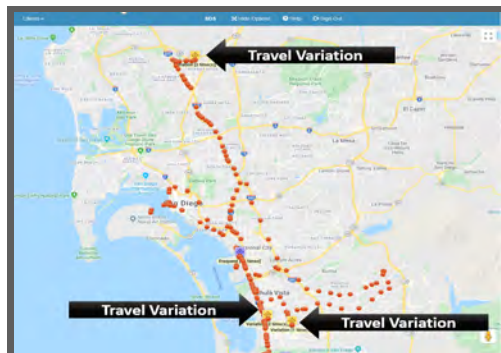
P | 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

POINT PATTERN ANALYSIS WITH DATA ANALYTICS

Point Pattern Analysis (PPA) for SentinelDNA delivers a comprehensive view of participant travel patterns throughout the community.

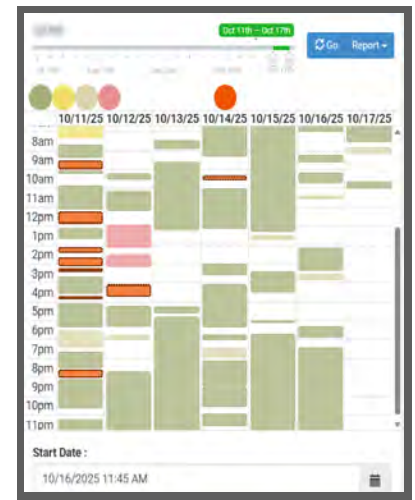
With larger and larger caseloads, field officers don't have the time to sift through thousands of GPS data points every day.

PPA provides visual queues that enable officers to quickly identify variations in participant travel patterns. These variations help supervising officers zero in on travel exceptions and address potential violations before they happen.



Locations a participant visited are analyzed and mapped. The number and duration of visits are displayed, enabling supervising officers to zero in on travel variations.

The calendar view in SentinelDNA shows approved locations and any travel variations.



ESSENTIAL FEATURES

- Streamlines Data Review by reducing the time spent reviewing thousands of GPS data points and brings attention to travel exceptions
- Increases Officer efficiency by reviewing 7 days of location information at one time
- Facilitates early intervention by recognizing changes in travel patterns for immediate officer response
- Customized labels can be assigned to known and variation locations
- Distinguishes variations and known locations using color-coded icons both on the calendar view and the map view
- Calculates the number of times visited and the total time spent at every location



SentinelDNA is the intelligent offender management platform with advanced analytics. SentinelDNA provides single-screen access to our comprehensive set of products and services.

GPS and RF Electronic Monitoring * Remote Alcohol Testing * Substance Abuse Screening
Domestic Violence Monitoring * Cognitive Skills Training * Full-Service Offender Management.

Call today to request a free demonstration or customized solution.

P| 800 589 6003 | SALES@SENTINELADVANTAGE.COM | WWW.SENTINELADVANTAGE.COM

Voice biometrics is a technology that uses a person’s voice to authenticate their identity. It works by analyzing the unique characteristics of a person’s speech, such as speed, accent, tone, pitch, etc., and creating a voice-print or voice template. When a person speaks again, their voice-print is compared to the stored samples to verify their identity.

HIGHLIGHTS INCLUDE:

- Biometric Verification
- Documented within the ShadowtrackONE Platform

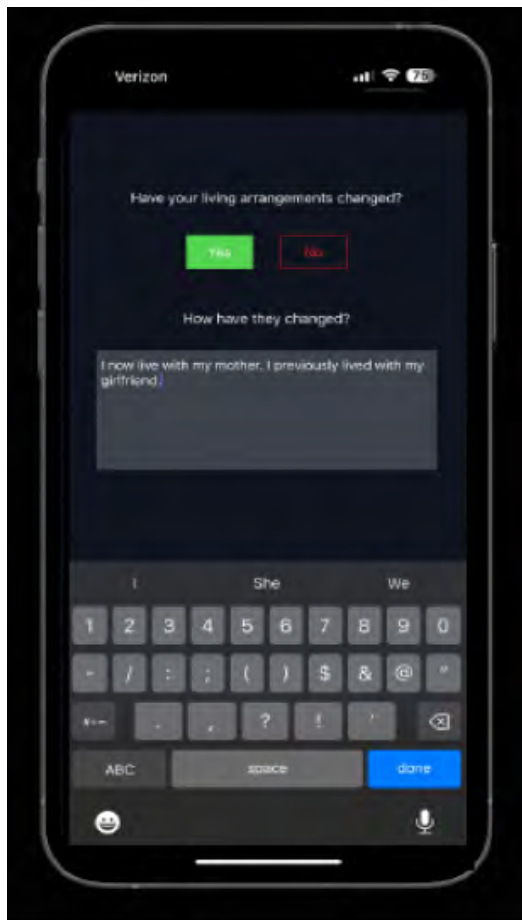


SPECIFICATIONS	
Verify Enrollee Identity	✓
Obtain a Location During Verification	✓
If Voice Fails Facial Is Initiated	✓
Officer Notified if Voice Fails	✓
Paired with Curfew & Interview Schedules	✓
Enrollee Repeats Three Phrases	✓
Enrollees can Perform Verifications at any time	✓
Anti-Spoofing Technology Built-in	✓

Our virtual interview solution provides an efficient and easy way for enrollees to report on a set schedule. Officers are made aware of enrollee location and any exceptions noted.

HIGHLIGHTS INCLUDE:

- Easily Obtain Updated Information
- Biometric Verification



SPECIFICATIONS	
Automated Interview	✓
Configurable Questions	✓
Officers Determine Interview Frequency & Number of Questions	✓
Agency/Officer Initiated Only	✓
Biometric Verification Required	✓
Enrollee Location Obtained	✓
All Answers Documented within the ShadowtrackONE Platform	✓
Officers Notified of Exceptions	✓
All Interviews Date & Time Stamped	✓
Caseload Management Integration	✓

ShadowLocate works in conjunction with all of the ShadowTrack services. Verifying the enrollee's location on a random or on-demand basis.

Devices:

- Enrollee App
- Officer App
- Officer Web Portal

SPECIFICATIONS

Verify Enrollee Location on Demand



Verify Enrollee Location on a Random Basis



Obtain Location via a Silent Request



Obtain Location via Facial Recognition



Obtain Location via Voice Biometrics



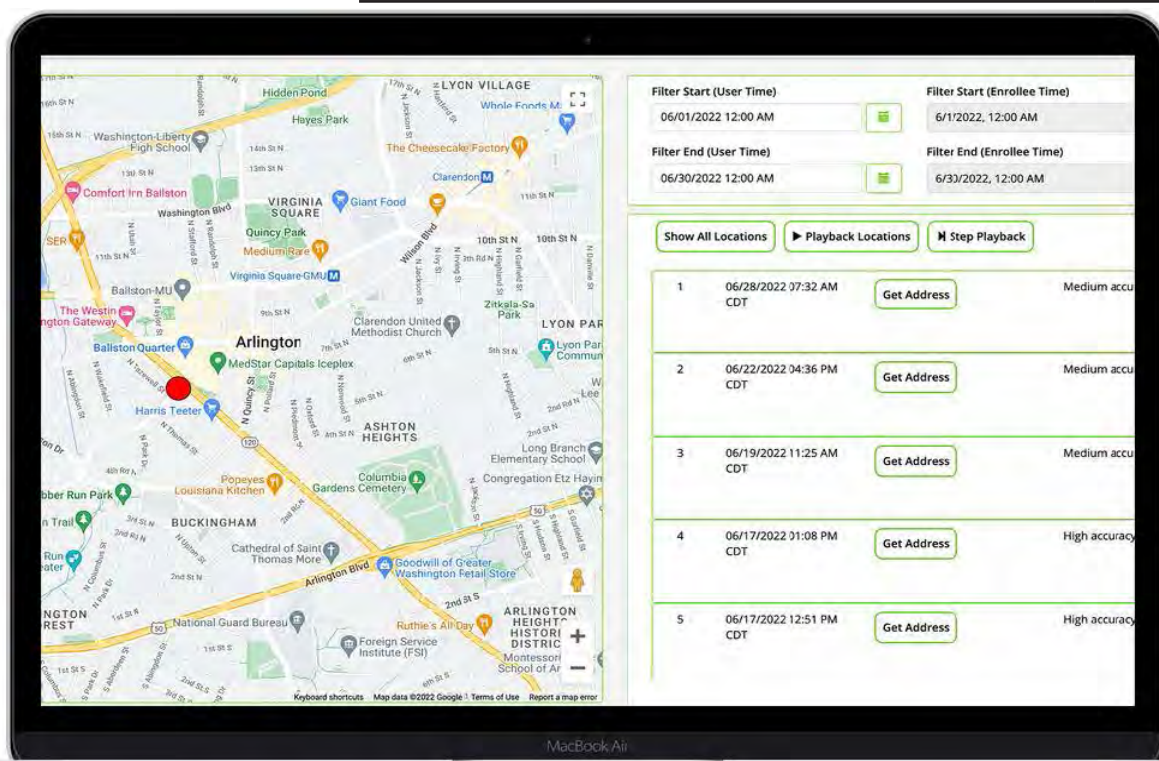
Obtain Location via Fingerprint Verification



Obtain Location Requests with Schedules



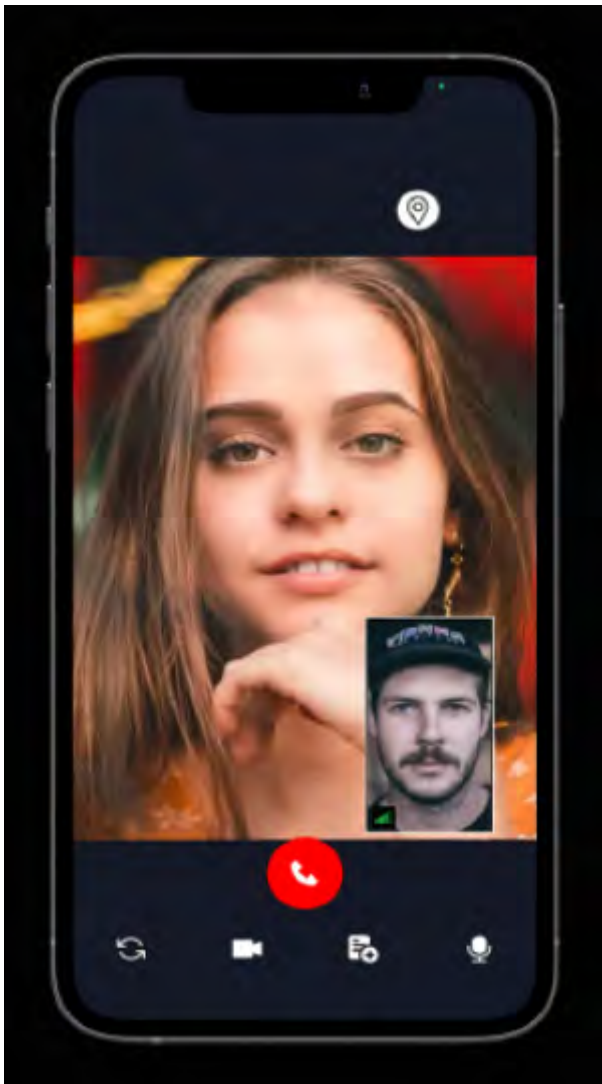
Caseload Management Integration



ShadowView is a two-way video session initiated by the officer.

HIGHLIGHTS INCLUDE:

- Officer Initiated
- Enrollee Location Obtained
- Call Details Documented Within Enrollee Profile



OFFICER SIDE	
Two-Way Virtual Communication	✓
Enrollee Location Displayed During Video	✓
Perform Home Contacts Virtually	✓
Enter Notes During or After a Video Call	✓
Protects Officer Time & Resources	✓
Schedule Virtual Appointments through our Calendar System	✓
Officer Initiated Only	✓
Ability to Mute Microphone	✓
Ability to Turn off and Flip Camera	✓
Ability to determine enrollee's signal strength	✓
Caseload Management Integration	✓
ENROLLEE SIDE	
Allows for Virtual Contact with Officer, thus Saving Time & Resources	✓
Appointment Reminders sent via our Calendar System	✓
Ability to Mute Microphone	✓
Ability to Turn off & Flip Camera	✓