

SECURUS

Monitoring™

an aventiv company

**NASPO VALUEPOINT
ELECTRONIC MONITORING
STATE OF NEVADA
CATEGORY 3: ALCOHOL MONITORING
SOLICITATION NUMBER 99SWC-S3474**

FEBRUARY 26, 2026

An RFP Solution Prepared for:

State of Nevada
NASPO ValuePoint
Chuy Ampudia,
Purchasing Officer
campudia@admin.nv.gov
775-531-3305

Presented by:

Securus Monitoring, an Aventiv/Satellite
Tracking of People LLC company
Kevin Elder, President
5353 W Sam Houston Parkway North, Suite
190
Houston, TX 77041
972-277-0300

TABLE OF CONTENTS

COVER LETTER: CATEGORY 3 ALCOHOL MONITORING GPS	2
OFFEROR RESPONSE WORKSHEET	4
I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS	4
II. RESPONSE TO TECHNICAL CRITERIA	5
C. Scope of Work – Category 3: Alcohol Monitoring GPS	6
D. Customer Satisfaction.	29
SCOPE OF WORK	48
I. Background and Definitions	48
II. General Contract Requirements. (Applies to all categories)	53
III. Information Technology Security Requirements. (Applies to all categories)	55
VI. Category 3: Alcohol Monitoring.	62
A. CAM or TAC	62
B. Remote Alcohol Monitoring (RAM)	76
EXHIBIT 1: AVENTIV NIST ATTESTATION LETTER	89

COVER LETTER: CATEGORY 3 ALCOHOL MONITORING GPS



February 25, 2026

State of Nevada/NASPO ValuePoint

Chuy Ampudia
Purchasing Officer
campudia@admin.nv.gov
775-531-3305

Re: NASPO ValuePoint RFP – Electronic Monitoring – Alcohol Monitoring

Dear Chuy Ampudia and NASPO ValuePoint Evaluation Committee Members,

Securus Monitoring (Securus), an Aventiv / Satellite Tracking of People, LLC company, respectfully submits this proposal in response to the recent NASPO ValuePoint Request for Proposals for Electronic Monitoring, with the State of Nevada serving as the sponsoring state. We appreciate the opportunity to support NASPO ValuePoint Participating Entities with proven, reliable, and innovative electronic monitoring solutions that enhance public safety while supporting effective community supervision.

Alcohol monitoring is an essential tool for agencies responsible for supervising individuals whose history of alcohol-related offenses, and potential continued use, may pose a risk to the surrounding community. Securus understands the responsibility that accompanies this mission and has designed its technology, services, and operational support to meet or exceed the rigorous expectations of agencies ranging from larger statewide programs to smaller county and municipal programs.

WHAT WE OFFER

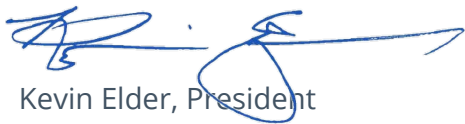
- **SoberTrack** - our state-of-the-art remote breath-alcohol concentration (BrAC) testing solution provides law enforcement and community corrections agencies with the ability to conduct scheduled and on-demand alcohol testing of participants regardless of their location.
- **SCRAM Continuous Alcohol Monitoring®** - We partner with SCRAM to provide 24/7 transdermal alcohol monitoring for clients with court or mandates of continuous alcohol monitoring (CAM). SCRAM's device is the most widely used and the only scientifically proven and court-validated device of its kind.

Securus is the original equipment manufacturer (OEM) of SoberTrack. Our ISO 9001:2015-certified assembly and manufacturing operations are based in Houston, Texas. We also own, operate, maintain, and continuously enhance VeriTracks, our customizable monitoring platform, which is updated at least three (3) times per year. As the OEM and system operator, Securus maintains full control over product quality, availability, and innovation to ensure Participating Entities are supported as program needs evolve.

Securus has provided all required forms, acknowledgements, and supporting documentation in accordance with NASPO ValuePoint and State of Nevada RFP instructions, including all issued addenda and certificates of insurance.

We value our longstanding partnership with NASPO ValuePoint and look forward to continuing to deliver dependable cutting-edge products, responsive support, and industry expertise that Participating Entities rely on every day. Thank you for your consideration of this proposal.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Kevin Elder', with a stylized flourish extending to the right.

Kevin Elder, President
Securus, An Aventiv / Satellite Tracking of People, LLC Company
5353 W. Sam Houston Parkway North, Suite 190
Houston, TX 77041
Phone: 682-444-8895
Email: kevin.elder@aventiv.com

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is the original equipment manufacturer (OEM) of all proposed equipment and software except for the wrist wearable, and our partner Talitrix is the OEM and SCRAM CAM. Our assembly and manufacturing operations are ISO 9001:2015-certified and based in Houston, Texas. Additionally, we own, operate, maintain, and enhance VeriTracks throughout the year, adding new features and functionality to meet the evolving needs of our partner agencies.

Government agencies at the federal, state, county, and municipal levels, as well as numerous non-government organizations, have relied on our electronic monitoring products and services to confidently and successfully monitor program participants of all types for more than 20 years. Securus continues to enhance its functionality based on the feedback of customers and their needs.

The proposed equipment has been used for active monitoring well beyond the three (3) year requirement. Securus has a longstanding record as the prime contractor for electronic monitoring services across agencies of varying sizes and risk profiles. Our experience includes supporting large jurisdictions supervising more than 9,500 participants as well as smaller agencies with only a limited number of individuals under monitoring. In every instance, Securus delivers consistent, high-quality service, scalable program management, and reliable technology designed to meet each agency's operational, compliance, and public-safety requirements.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Please see **Scope of Work** within this document for Securus' response.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is proud to provide nationwide services including (Hawaii and Alaska). We also currently offer services outside of the United States in Mexico and Canada.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Please see **Attachment 02 - Section III** within this document for Securus' response.

II. RESPONSE TO TECHNICAL CRITERIA

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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)

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Please see below answers for Scope of Work for Category 3: Alcohol Monitoring.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus will be offering SoberTrack and SCRAM for Alcohol Monitoring:

SoberTrack

SoberTrack Equipment Specifications

- Dimensions: 5.5" x 3" x 1.3"
- Weight: Approximately 9 ounces
- Battery Type: Lithium-ion
- Case Material: Industrial-grade hypoallergenic plastic
- Environmental Conditions: Operates from 5 – 120 degrees Fahrenheit, 0- 90% humidity
- Alcohol Detection Technology: Fuel cell, DOT approved
- Number of Hours Single Battery Charge Powers the Unit: 48+ hours
- Length of Time to Recharge the Unit's Battery: 2 hours
- Battery Life: 24 months
- Method for Confirming Client's Identity: Still-photo comparison
- Method for Notifying Client of a Test: Tone
- Frequency of Administering Tests: On-demand, random, and scheduled
- Frequency of Test Results Reporting: Immediately after test



- Time interval for retesting after a failed test: 10 minutes
- Frequency of Receiving GPS Location Points:
 - Once every minute while testing starting at 10 minutes before the test and ends 10 minutes after the test
- Logs and reports one (1) GPS track point every hour when left idle
- Ability to temporarily turn on tracking by the field officer through VeriTracks
- Cellular Networks Used for Reporting: AT&T and T-Mobile
- Tamper Detection: Light sensor within device

Power Supply

SoberTrack contains a lithium-ion battery that will maintain its charge for 48+ hours. To recharge the unit's battery, Securus recommends a charge time of two (2) hours. It has a sealed battery that lasts for 24 months and does not require field installation or service of the battery. Notifications alerting the supervising officer of the battery status are provided 30 days in advance to ensure the supervising officer has time to switch out the device. If a device has not been properly charged, it can go into a Low Battery Status. This generates an alert to the supervising officer; however, the device will continue to operate for up to ten (10) hours. This allows time to have the client charge the device, continuing participation in the program. SoberTrack will also provide tone alerts to remind the client of the need to charge the device.

SCRAM



The SCRAM Continuous Alcohol Monitoring® (SCRAM CAM®) 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.

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. SCRAM CAM:

- Encourages compliance because it eliminates testing gaps—meaning that there is no way to miss a test or drink around testing schedules.
- Uses a controlled, quantifiable sample, resulting in true continuous monitoring and the lowest false positive rate possible.
- **Battery life of 90+ days** significantly reduces the need for constant communication and supervision.

- 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.
- Is court-validated—meaning 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.

As the pioneer of CAM technology, SCRAM Systems launched the original Secure Continuous Remote Alcohol Monitor (SCRAM) system to the criminal justice market in 2003. In 2010, optional, built-in RF house arrest capabilities were added to the bracelet to provide dual functionality. Known today as SCRAM CAM, it is part of the SCRAM Systems line of electronic monitoring and corrections software solutions. SCRAM CAM has monitored more clients worldwide than all other transdermal devices combined.

3. Describe your software system (web-based applications, smart phone applications). Describe unique design features that ensure accuracy and/or speed of reporting.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

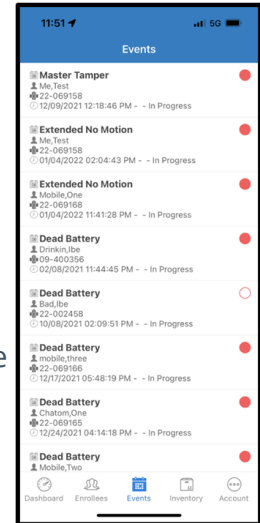
Securus offers VeriTracks, our web-based monitoring software to support enrolling, tracking, and viewing activities of clients. Securus' devices utilize the same monitoring software so there is no switching between monitoring applications. VeriTracks is 100% web-based, meaning that Participating Entity does not download any software onto its IT network or individual computers. Participating Entity-authorized personnel login to VeriTracks using any computer, laptop, smart phone, or tablet with a high-speed Internet connection.

Enrollink

Securus provides the VeriTracks Mobile application to support supervision on-the-go. The free VeriTracks Mobile app is available in the Google Play or iOS App Store and provides an additional tool for supervising clients when a laptop is not readily accessible. The

VeriTracks Mobile app and VeriTracks, the web-based monitoring application, interact with each other and immediately synchronize data.

Authorized Participating Entity personnel can complete many of the standard caseload management tasks, including enrolling and un-enrolling clients, installation and removal of equipment, inventory scans for equipment, confirming and closing events, adding client photos and narrative-style notes about an event or the client, etc. The Dashboard in VeriTracks Mobile is like the standard version of VeriTracks, so field personnel can immediately see if any client has an open event, check the battery condition of any given subject's device, etc. They can also initiate BLUtag commands, such as requesting the location of a device and emit an audible tone or vibrate the device.



VeriTracks Mobile offers the Pursuit function, which is like Rapid Reporting. In Pursuit mode, BLUtag receives a GPS location point once every 15 seconds and reports into VeriTracks every 60 seconds. Due to the frequent display of the location points, the client's direction of travel is immediately visible. Officers can also see the distance between themselves and the client.

VeriTracks Mobile utilizes SHA-256 Cryptographic Hash Algorithm and Two Factor Authentication to support security of customer data.



Securus also offers client applications (ENROLLINK) to support schedule change requests and update their photos within VeriTracks, upon supervision staff approval. The supervision staff can perform video calls and recorded, text-based communication to the client through VeriTracks. ENROLLINK can be used to receive additional information from the client including random GPS checks through location requests and the requirement to contact the assigned supervision staff. When initiated, the client will receive a notice on their phone to perform the Location Verification and additional instructions can be provided to them upon completion.

Mobile Application for Enrollees: ENROLLINK®

ENROLLINK® is a smartphone application developed specifically for monitored individuals to support secure, two-way communication and data submission. ENROLLINK allows enrollees to:

- Request schedule changes for staff review and approval
- Submit photos and location verification data

- Receive messages, instructions, and requests from supervising staff

All ENROLLINK interactions are transmitted into VeriTracks, ensuring that enrollee-submitted information is captured directly in the system of record without manual data entry.

To ensure accuracy, ENROLLINK incorporates proprietary facial recognition technology during registration and subsequent logins by comparing stored enrollee images with newly captured images. This design feature helps verify the identity of the individual submitting data through the application.

Design Features Supporting Accuracy and Speed of Reporting

Single, Integrated Platform: VeriTracks, VeriTracks Mobile, and ENROLLINK operate within a unified system, eliminating delays or errors associated with transferring data between systems.

Real-Time Synchronization: Data entered through mobile applications synchronizes immediately with the web-based platform, supporting timely reporting and up-to-date visibility.

Automated Data Capture: GPS data, events, photos, and enrollee interactions are captured electronically and stored directly in VeriTracks, reducing reliance on manual reporting.

High-Frequency Location Reporting: Pursuit Mode increases reporting frequency to support rapid response and accurate event documentation.

Identity Verification: Facial recognition within ENROLLINK supports data integrity by validating the identity of the enrollee submitting information.

Securus's integrated web-based and mobile software ecosystem enables real-time data capture, rapid synchronization, and automated reporting, supporting accurate and timely supervision and court-ready documentation.

SCRAM

SCRAM Systems utilizes **SCRAM Optix™**, its proprietary, **web-based monitoring platform**, as the centralized system for managing electronic monitoring programs. SCRAM Optix is accessible 24/7 through any standard web browser and does not require software installation on agency networks or individual workstations. Authorized users access the system through role-based permissions established by the agency, enabling secure control of data visibility and system functions.

Through SCRAM Optix, authorized personnel can enroll clients, configure supervision parameters, manage GPS schedules and zones, review alerts, access historical and current monitoring data, and generate reports. The platform supports management of multiple SCRAM technologies within a **single unified dashboard**, allowing agencies to monitor their caseload without switching between systems.

SCRAM Optix also supports customizable reporting and audit logs, allowing agencies to retrieve monitoring records for court review and evidentiary purposes, consistent with chain-of-custody requirements.

Smartphone and Mobile Applications

SCRAM Systems offers multiple mobile-enabled solutions that integrate with SCRAM Optix:

- **SCRAM TouchPoint®** is a **participant-facing mobile application** available on iOS and Android devices. TouchPoint provides secure messaging, automated reminders, check-in functionality, and biometric identity verification using supported mobile device capabilities. Data collected through TouchPoint integrates directly with the SCRAM monitoring ecosystem.
- SCRAM Optix is **mobile-adaptive**, allowing officers and authorized personnel to securely access monitoring data, alerts, and client information from smartphones or tablets using a web browser, without loss of core functionality.
- **SCRAM Ally®** is a victim-notification mobile application that works in conjunction with SCRAM GPS to notify victims and supervising authorities when proximity thresholds are breached, without requiring the victim to carry a GPS device.

Design Features Supporting Accuracy and Speed of Reporting

SCRAM's software ecosystem is designed to support **timely, accurate reporting** through the following documented features:

- **Unified Platform Architecture:** All SCRAM monitoring technologies report into SCRAM Optix, reducing data fragmentation and ensuring that alerts, location data, and event histories are processed and displayed within a single system.
- **Flexible Zone and Schedule Configuration:** SCRAM Optix supports inclusion, exclusion, buffer, and neutral zones with customizable schedules, allowing accurate correlation of location data to supervision rules defined by the agency.
- **Alert Management Controls:** Authorized users can configure which events generate alerts, how alerts are delivered, and which personnel receive notifications, supporting efficient review and response workflows.
- **Biometric Verification (Mobile Solutions):** SCRAM TouchPoint incorporates biometric identity verification through supported mobile devices, helping ensure

that reported check-ins and mobile interactions are associated with the correct individual.

- **Secure, Centralized Data Management:** Monitoring data is collected, analyzed, and stored within SCRAM's centralized system, allowing near real-time visibility of events and reducing delays associated with manual data reconciliation.

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.

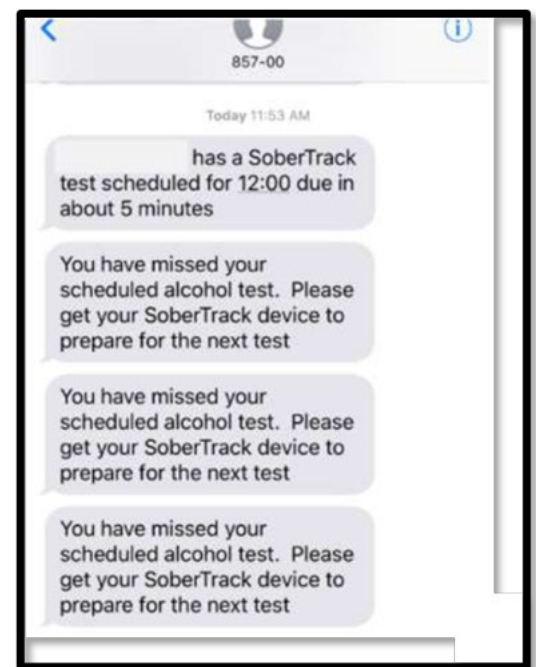
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus offers both SoberTrack and SCRAM alerts:

SoberTrack Notifications

VeriTracks will generate an alert for missed or failed tests and failure to pass facial recognition. Participating Entity supervisors can establish variable options depending on local mandates for a client's situation. These options include setting the BrAC rate for a positive test from 0.01 to 0.04, as well as the number of retests allowed before a positive/missed/failed test alert is generated. Many agencies allow up to three retests prior to a violation alert to document failed attempts. This additional documentation can help supervising officers determine when to initiate a violation of the program.

When a client's mobile phone number is provided, a text message is sent to the client five (5) minutes prior to a scheduled test. If they miss or fail a test, and a retest is initiated by the device, an additional text message is generated. If the test is random and the client fails to take the initial test, a text message is sent to the client reminding them of a pending required test.



SCRAM Alert Notifications

Notification methods for all alerts include email, text, and/or a Daily Activity Plan (DAP). The DAP can be automatically delivered up to twice daily. 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.

House Arrest events can be selected as priority alerts, ensuring notification within 15 minutes of the alert either by email and/or text, as specified. Additionally, House Arrest events are integrated into the client-facing TouchPoint application, creating improved program efficiencies, and streamlining officer/client communications.

5. Describe your customizable reporting. How does the reporting work with court requests and chain of custody requirements for legal purposes.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

VeriTracks can produce standard and ad hoc reports.

VeriTracks contains more than 300 reports and when Participating Entity-authorized personnel login to the web-based application, they can generate reports reflecting real time data. Reports can be sorted or filtered using any field. They can also be filtered to reflect data for a single supervising officer, a single office or division, a group of supervising officers, a geographic region of offices or counties or the entire Participating Entity' program. VeriTracks automatically stores a copy of each generated report for future reference. Participating Entity-authorized personnel can print reports from the screen or export them in several common formats, including Microsoft Word and Excel, PDF and comma delimited.

The Participating Entity can restrict access to certain reports. For example, VeriTracks contains a wide variety of reports related to program management. The Participating Entity may want to restrict access to these reports to program administrators who can generate them.

The VeriTracks reporting subsystem provides a great deal of customization to support a particular Participating Entity' requirements. While an initial standard template of reports is delivered to set up a Participating Entity's database, the database supports the addition of reports developed specifically for the Participating Entity. These reports may replace existing reports within the template or represent additions. Reports not required by the Participating Entity may be removed from the template.

Customizations include changing any aspect of the report format to include insertions of a Participating Entity' logo (thereby superseding the standard Securus logo), re-arranging data element and label placement, etc.

Due to the volume of data referenced by many of VeriTracks reports, our custom report writing group facilitates the process of customizing reports for customers. Customizing

reports is a very straightforward process, does not require a custom release of the software and can very easily be initiated at the request of a customer.

Reports are customizable by filtering or sorting on any field(s). They are exportable in a variety of formats (.pdf, .xls, .doc, etc.). Developing new custom reports or adjusting to existing reports can be completed at no additional cost to the Participating Entity by our report writing team.

Court-Requested Reporting and Chain of Custody

Securus follows forensic evidence handling procedures in that:

- Monitoring data is captured electronically within a secure system
- Access is limited to authorized personnel
- Reports are generated directly from system-recorded data
- Reporting follows Participating Entity and court-defined procedures

Accordingly, Securus supports court use by preserving system-generated records and controlled access, while the Participating Entity remains responsible for submitting reports and satisfying jurisdiction-specific evidentiary or chain-of-custody requirements.

Securus supports court reporting requirements by securely capturing and maintaining monitoring data within its web-based platform and generating reports in accordance with Participating Entity protocols, while final evidentiary handling and chain-of-custody determinations remain subject to court and jurisdictional requirements.

SCRAM Reporting

SCRAM Optix 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. Reports can be customized and tailored to best suit the Participating Entity's needs, further helping to reduce officer workload.

SCRAM Court Support Program

SCRAM Systems provides the most comprehensive Court Support Program in the industry. Since 2003, SCRAM Systems has worked with courts and ancillary agencies to provide comprehensive SCRAM CAM testimony, which has included the creation of more than 3,600 formal court reports used to detail the monitoring results of clients who denied a SCRAM

CAM violation (either alcohol consumption, equipment tampering, or a combination). In most cases, clients confronted by the court armed with a comprehensive SCRAM CAM reporting package admitted to the violation prior to the scheduled hearing. SCRAM Systems supports our technology in courts at every level and provides everything from a written report confirming a violation to in-person expert testimony for evidentiary hearings.

What Are Frye and Daubert?

Frye v United States was a 1923 case that challenged that new, legitimate scientific evidence was being wrongly omitted as evidence. The U.S. Supreme Court ruling in the case established what is known today as the **Frye Standard**, which states that scientific conclusions must be “generally accepted” within the scientific community in order to be admitted as evidence in a court of law.

In 1993, the U.S. Supreme Court issued a ruling in ***Daubert v Merrill Dow Pharmaceuticals*** that paved the way for what is now considered the most stringent standard for the admissibility of scientific evidence and testimony. The goal of the ruling was to establish a standard that helped courts to balance the admissibility of legitimate, cutting-edge scientific evidence while also limiting evidence based on “junk science” that has not been properly vetted for admissibility.

Today, some states apply the Frye Standard, some the Daubert Standard, and some a hybrid of the two.

SCRAM CAM is the only transdermal alcohol monitoring device to meet and exceed both of these standards for admissibility in multiple states and to the state Supreme Court level. The acceptance of SCRAM CAM as peer-reviewed and court-validated does not extend to other transdermal alcohol monitoring technologies.

6. Describe your Customer Service, including at least the following:

a. Hours of operation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Our Solutions Center provides Monitoring Center service and technical support to customers 24 hours a day, 365 days a year. It is housed in our Houston, Texas,

headquarters and staffed only with Securus employees who are on-duty rather than on-call regardless of the shift. Participating Entity-authorized personnel can access this resource through a toll-free phone number and email.

Our Solutions Center technicians also provide Monitoring Center service, where we receive notification of events generated by the clients in the Participating Entity' community such as unauthorized absences, late arrivals, equipment malfunctions, and tampering. Our technicians provide Monitoring Center service 24 hours a day, 365 days a year, and manage the events by following the protocols provided by the Participating Entity. The Monitoring Center service is customizable to meet the Participating Entity' evolving needs. For example, we can receive all event notifications or only those designed by the Participating Entity.

SCRAM

SCRAM Systems provides **customer service and monitoring center support 24 hours per day, 7 days per week, 365 days per year**. The monitoring center is fully staffed at all times by trained SCRAM Systems personnel who support real-time monitoring, alert analysis, technical assistance, and customer inquiries. Customer service is continuously available via **tollfree telephone access**, as well as email and web-based channels, ensuring uninterrupted support for Participating Entities regardless of time, day, or holiday.

b. Order procedures (how long to respond to order, delivery time frame). Delivery time after receipt of order? Describe online ordering procedures.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Upon receipt of an authorized order under the Master Agreement and applicable Participating Addendum, Securus processes orders during standard business hours, Monday through Friday, excluding holidays. Orders are reviewed for completeness and confirmed prior to fulfillment to ensure accuracy and compliance with Participating Entity requirements.

Securus's standard shipping policy is to process and ship orders within forty-eight (48) hours of receipt, Monday through Friday, between 8:00 a.m. and 3:00 p.m. Central Time, excluding holidays. Hardware is shipped using a third-party shipping vendor and expedited or next-day air shipping is available when required by the Participating Entity.

Securus maintains sufficient inventory of finished goods and consumables to support timely fulfillment and minimize delays.

Orders for Securus products and services may be initiated electronically in accordance with the Participating Entity's Participating Addendum. In addition, Participating Entities and authorized users access Securus services through VeriTracks, Securus's secure, web-based

application, which supports program administration and ongoing operational needs following order fulfillment. Ordering and service activation are coordinated by Securus's account management team to ensure proper onboarding and timely commencement of services.

SCRAM

SCRAM Systems maintains sufficient inventory to support Participating Entity needs and processes equipment orders **promptly upon receipt**. Orders placed **before 3:00 p.m. Mountain Time** are **shipped on the same business day** using standard delivery methods. Order coordination may be completed through the Participating Entity's **dedicated account manager** or by contacting SCRAM Systems Customer Service.

Delivery Time After Receipt of Order:

Standard equipment orders are shipped using **standard three-day delivery at no additional cost** to the Participating Entity. When urgent or unanticipated needs arise, **overnight or next day delivery** can be arranged upon request. In the event of equipment malfunction or maintenance requiring return, SCRAM Systems issues a **Return Merchandise Authorization (RMA)** and ships a replacement device immediately, typically ensuring replacement equipment is received **within 24 hours**.

Online and Electronic Ordering Procedures:

SCRAM Systems supports streamlined ordering and inventory management through **SCRAM Optix®**, the secure, web-based platform that allows authorized personnel to **view inventory status, track devices, and coordinate replacement or additional equipment needs**. Orders and requests may also be initiated electronically through Customer Service or the assigned account manager, enabling efficient tracking and documentation of all equipment transactions.

c. Product request response time (what is kept on hand at office vs ordering products) – inventory on hand.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus maintains **inventory of SoberTrack devices and consumables** to support timely fulfillment of Participating Entity needs and to minimize operational disruptions. Devices returned from the field are **tested and verified prior to being placed back into inventory**, ensuring all equipment issued is fully functional and calibrated for use.

OnHand Inventory:

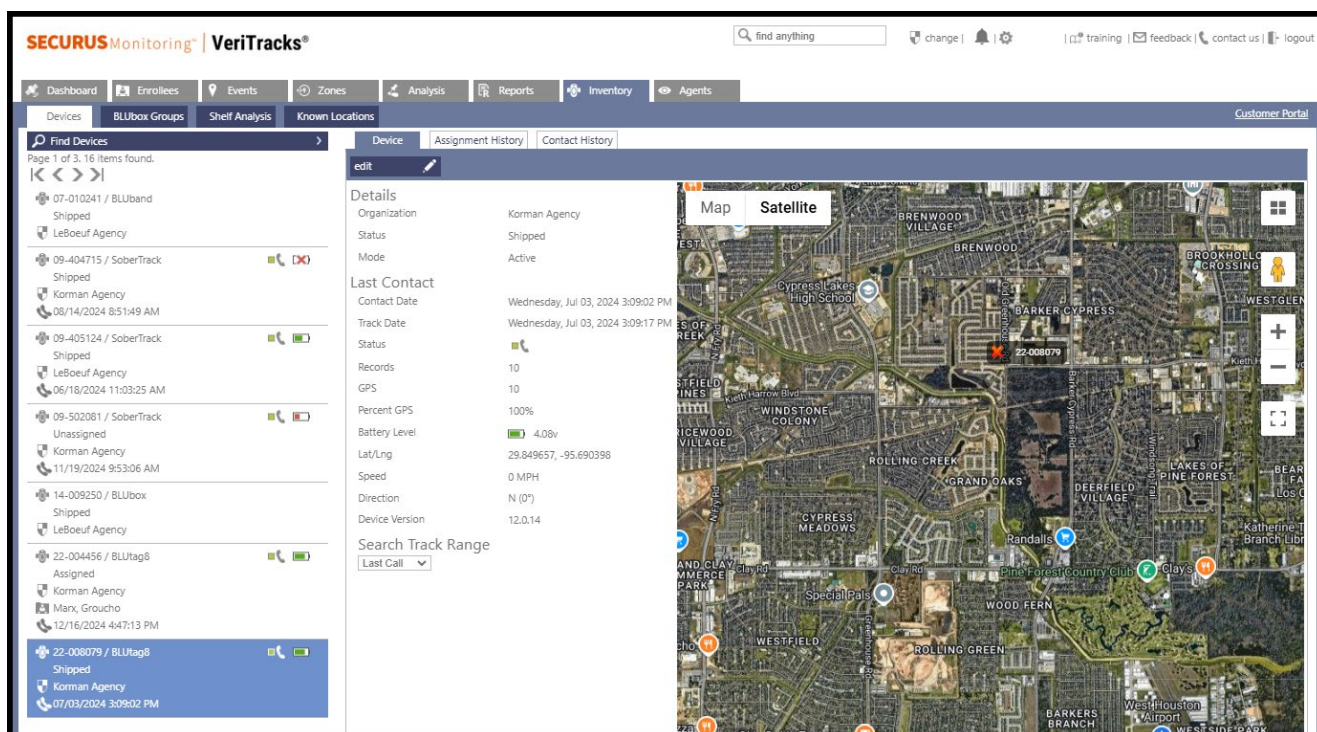
Participating Entities may maintain **local on-hand inventory** to support immediate deployment and routine device swaps. Securus works collaboratively with each agency to establish appropriate inventory levels based on program size, usage patterns, and anticipated demand.

Product Requests and Replacements:

When additional SoberTrack devices are required—due to program growth, device replacement, calibration cycles, or damage—Securus fulfills orders from **central warehouse inventory**. Replacement or additional devices are **typically shipped promptly upon request**, allowing agencies to maintain continuity of services. Devices requiring recalibration are proactively identified within VeriTracks, and replacement units are provided in advance of calibration expiration.

As the **original equipment manufacturer (OEM)**, Securus controls assembly, testing, and distribution of SoberTrack devices, enabling rapid response to Participating Entity requests and ensuring consistent product availability throughout the contract term.

Using VeriTracks, authorized personnel never have to wonder about the state of their available inventory. Within the Inventory Tile in VeriTracks, there is a recorded status of each piece of assigned equipment. If a given piece of equipment is not immediately found within the customer's inventory while logged into VeriTracks, the authorized user can also search for it using the "Find Anything" field, which displays on every page of VeriTracks.



The Inventory Tile in VeriTracks.

One of the most used reports in VeriTracks is the Inventory reports. This report lists the agency to which the equipment is assigned, the serial number, operating mode (if

applicable), who the device is assigned, and status. This report enables field personnel to track all client monitoring equipment usage by subject name, active status, lost (unrecoverable), returned (Needs Repair, Returned) over a specified time period. Additionally, this report enables field personnel to distinguish between monitoring equipment in use, equipment in inventory, and equipment returned for service.

SECURUSMonitoring® VeriTracks®			
Device Inventory Summary by Agency			
Collado Training Agency			
Collado Training Agency			
Product	Status		
BLUband	Assigned		1
BLUband	Shipped		2
BLUband	Unassigned		6
		Total Devices for BLUband	9
BLUbox	Shipped		1
		Total Devices for BLUbox	1
BLUhome Cellular	Assigned		1
		Total Devices for BLUhome Cellular	1
BLUscan	Shipped		2
		Total Devices for BLUscan	2
BLUtag8	Assigned		7
BLUtag8	Unassigned		4
		Total Devices for BLUtag8	11
SoberTrack	Assigned		4
SoberTrack	Unassigned		2
		Total Devices for SoberTrack	6
StalkerAlert	Unassigned		1
		Total Devices for StalkerAlert	1
		Total Devices for Collado Training Agency	31
		Assigned	Unassigned
Blutag :		0	0
Blutag2 :		0	0
Blutag8 :		7	4
Blu+ :		0	0
Report Filename: D:\Presentation Server\processor\reports\Device_Inventory_Summary_by_Agency_Report_128.rpt			
Report Date: 12/18/2024 17:16:37		Page 1 of 1	

The Device Inventory report lists all the equipment assigned to this sample agency. It provides the status of each piece of equipment and, if assigned, the client's name and ID number.

Our reporting section, or Inventory Tab, allows reports to be run showing active inventory and those devices that were returned to the Securus Houston, Texas manufacturing facility. This can be used to do a physical count of devices in the customer's inventory.

While these reports can be easily displayed within VeriTracks, or set to deliver through email on a daily, weekly, monthly, or quarterly basis to designated recipients, our Solutions Center technicians are also available to help understand the data and/or monitor the inventory as well.

Upon award, our dedicated Account Manager will work with Participating Entity to create an Inventory Plan, with reporting, which meets the needs of the electronic monitoring program.

SCRAM

SCRAM Optix® provides Participating Entities with the ability to manage and track inventory through a centralized, web-based platform. Authorized users can view device status, monitor inventory levels, and manage equipment assignments in real time.

To support uninterrupted program operations, Securus maintains established fulfillment processes to ensure that replacement or additional equipment is shipped promptly following notification or order placement. New products are typically dispatched within forty-eight (48) hours, subject to standard shipping terms and availability.

7. How do you comply with local and state regulations (what type of research do you conduct when working with a new entity?)

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

As an industry leader, we must evolve with the always-changing regulatory climate. To do so, we maintain internal legal and regulatory departments so the products and processes used by our clients are compliant and effective with all emerging trends and regulatory changes that can impact the market. We stay up to date on changes so you can stay up to date with the market.

Securus complies with all applicable federal, state, and local laws and regulations. We comply with both NIST and FIPS standards to ensure network, application, data transmission, data storage, and physical security. We also comply with all HIPAA laws to protect all user, enrollee, and victim data. Securus submits to annual audits and safety inspections, and we maintain our ISO 9001:2015 certification (recently renewed through December 2026). As our customers' needs change, we implement new laws and regulations at no additional expense. For example, in the domestic violence area, we have adapted our security measures and released new products to support continued community safety.

When engaging with a new Participating Entity, Securus conducts structured, front-end research during the Program Management phase to ensure the electronic monitoring program is configured to meet the entity's legal, operational, and technical requirements.

Immediately following contract award, Securus works directly with the Participating Entity to review existing program structure, policies, and procedures, including supervision models, participant workflows, escalation protocols, and reporting requirements. This research establishes a clear understanding of how the entity currently operates its monitoring program and identifies any entity-specific requirements that must be incorporated into implementation.

Securus evaluates the Participating Entity's technical environment and infrastructure, including connectivity needs, system access levels, user roles, and security requirements. This assessment supports proper configuration of VeriTracks, Securus's web-based monitoring platform, and ensures system settings, notification preferences, and reporting tools align with agency operations.

As part of onboarding research, Securus reviews the Participating Entity's staffing model and training needs. Training curricula are assessed and customized as necessary to reflect the entity's monitoring protocols, program scale, and user roles. Training schedules, delivery methods, and equipment deployment quantities are confirmed based on this research.

Securus also accounts for applicable legal, regulatory, and program-specific requirements impacting electronic monitoring operations. This includes ensuring compliance with relevant laws, standards, and security requirements applicable to the Participating Entity's program and jurisdiction.

8. Describe the on-boarding process for new Participating Entity.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus follows a **structured, collaborative on-boarding process** to ensure smooth and efficient implementation of **SoberTrack®** for new Participating Entities. The process is designed to minimize disruption to existing operations while ensuring agency staff are fully trained and supported.

Phase 1: Program Planning and Configuration

Following contract award, Securus works with the Participating Entity to define program requirements, operational protocols, reporting preferences, and inventory needs. During this phase, system settings and alert thresholds are configured within **VeriTracks®**, and user roles and permissions are established for agency personnel.

Phase 2: System Setup and Equipment Preparation

Securus creates the Participating Entity's secure database and user accounts within VeriTracks. SoberTrack devices designated for initial deployment are **tested and prepared prior to shipment**. Equipment is delivered to designated locations in advance of training to allow for hands-on instruction and validation.

Phase 3: Training and Knowledge Transfer

Securus provides **comprehensive initial training** for agency designated personnel, covering both SoberTrack hardware and the VeriTracks monitoring platform. Training may be conducted **onsite or remotely**, based on agency preference, and includes hands-on enrollment, scheduling, test review, reporting, and inventory management. Follow-up, refresher, and new feature training are also available at no additional cost.

Phase 4: Go-Live and Operational Support

Once training is complete, the Participating Entity begins enrolling clients and conducting monitoring activities. During the initial operational period, Securus provides **enhanced technical support**, assisting with report review, alert management, and workflow optimization to ensure the agency is fully leveraging the system's capabilities.

Phase 5: Ongoing Support and Optimization

After implementation, Securus continues to support the Participating Entity through **24/7/365 technical support**, access to online training resources, and ongoing product updates. Inventory levels, device calibration cycles, and reporting practices are continuously supported to ensure long-term program success.

SCRAM

SCRAM Systems follows a **structured, collaborative on-boarding process** to ensure new Participating Entities are fully prepared to operate SCRAM alcohol monitoring programs efficiently, securely, and in compliance with jurisdictional requirements.

Phase 1: Program Planning and Configuration

Following contract award, SCRAM Systems works with the Participating Entity to review program objectives, staffing models, operational workflows, and applicable legal or regulatory requirements. During this phase, system configurations, notification preferences, reporting requirements, and user access roles are defined to align with agency protocols. This planning ensures the SCRAM Optix® platform is configured to support the Participating Entity's specific monitoring needs.

Phase 2: System Setup and Account Provisioning

SCRAM Systems establishes secure agency accounts within SCRAM Optix®, including user profiles, permission levels, and inventory tracking. Equipment quantities and delivery locations are confirmed, and deployment logistics are coordinated to support training and

initial operations. Any required data entry or transition preparation is completed to minimize administrative burden on Participating Entity staff.

Phase 3: Initial Training and Knowledge Transfer

SCRAM Systems provides **comprehensive initial startup training at no additional cost**, delivered onsite or remotely. Training covers enrollment of clients into the software system, installation, use, deinstallation, and cleaning of equipment, generation and interpretation of monitoring and compliance reports, and accessing technical support tools, help menus, and the 24/7 monitoring center. Training is customized based on user roles and program complexity, and all reference materials remain available online for refresher and new hire training.

Phase 4: Go-Live Support

Upon completion of training, the Participating Entity transitions to live operations. SCRAM Systems provides enhanced support during this period to assist with alert workflows, reporting, equipment usage, and operational questions. A dedicated account representative serves as the primary point of contact to ensure a smooth transition.

Phase 5: Ongoing Support and Optimization

After implementation, SCRAM Systems continues to support the Participating Entity through **24/7/365 monitoring and technical support**, access to SCRAM Systems University, ongoing training opportunities, and periodic program reviews. This ensures long-term operational success and continuous alignment with agency needs

9. Describe the on-boarding process for new Clients. Include any installation information that may apply.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus has established a **streamlined, efficient client on-boarding process** for individuals placed on **SoberTrack® alcohol monitoring**, designed to minimize administrative burden while ensuring clients clearly understand program expectations and device operation.

Client Enrollment and Account Setup

Authorized agency personnel initiate the onboarding process by creating a **client profile in VeriTracks®**, Securus's secure, web-based monitoring platform. Required identifying information, supervision details, and monitoring parameters—such as testing schedules, alert thresholds, and notification recipients—are entered at this time. Once the profile is created, the client is assigned to a SoberTrack device within VeriTracks, which becomes the system of record for all test results, alerts, and compliance history.

Device Assignment and Installation

SoberTrack is a **one-piece, handheld, GPS-enabled mobile breath alcohol monitoring device** and **does not require installation of any equipment in the client's residence**. There is **no base station, landline, or home receiver** required. The device communicates test results and location data directly to VeriTracks using nationwide cellular service.

Installation consists of issuing the SoberTrack device to the client, verifying the device is charged, and confirming cellular connectivity. The supervising officer or authorized staff reviews proper handling, charging requirements, and testing procedures with the client. Because there are no field replaceable parts and no home installation requirements, the process is completed quickly and consistently across client populations.

Client Orientation and Instructions

During on-boarding, clients receive clear instructions on:

- How and when breath tests will be conducted
- Proper use of disposable testing straws
- Charging requirements and battery notifications
- Photo capture and identity verification during testing
- Consequences of missed, failed, or tampered tests

Written instructions are provided, and testing schedules are stored both on the SoberTrack device and within VeriTracks to ensure the client receives timely prompts for required tests.

Activation and Go-Live

Once orientation is complete, the client begins monitoring immediately. Test results, GPS data, and alerts are transmitted to VeriTracks in near real time. Supervising personnel can monitor compliance, review test photos, and respond to events as they occur.

Ongoing Support

Throughout the supervision period, Securus provides **24/7/365 technical support** for agency personnel and assists with device replacement, calibration cycles, and client questions as needed. Clients do not need to return to an office for home equipment installation or removal, which further reduces barriers to compliance.

SCRAM

SCRAM Systems provides a **standardized client on-boarding process** that begins with creation of a client profile in **SCRAM Optix®** by authorized agency staff, capturing required identifying and supervision information prior to activation. Assigned SCRAM equipment is

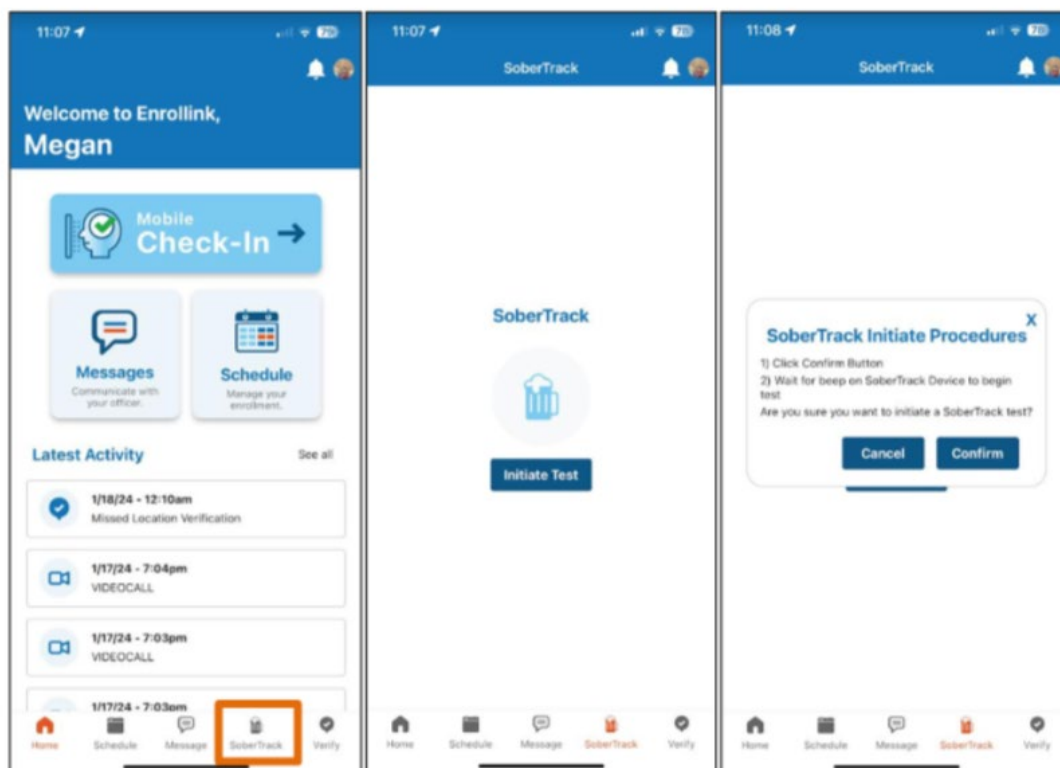
then **linked to the client record and installed** by trained personnel in accordance with manufacturer specifications to ensure secure, comfortable placement and proper data transmission. During installation, the client receives a **comprehensive orientation** covering program requirements, device care and maintenance, prohibited behaviors, and instructions for responding to alerts or equipment issues, along with **24/7 support contact information**. Monitoring is activated immediately following installation, with verification that communication and alert settings are functioning correctly, ensuring uninterrupted oversight from the start of supervision.

10. Provide screen shots showing the functionality and user experience of the web-based platform as well as the mobile platform.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack

Paring SoberTrack with Enrollink



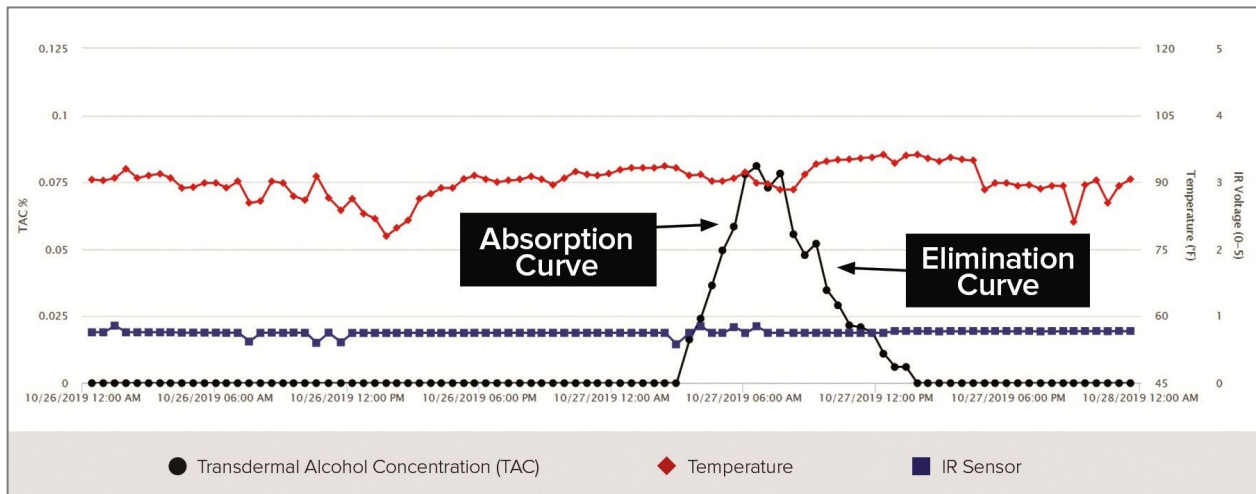
Test Review from SoberTrack Summary

SoberTrack Summary								
Review Tests								
	Type	Start Date	Result Date	Monitoring Result S...	BAC	Confirmed		
-	On Demand	02/03/2020 03:43:24 PM	-	In Progress	0	Not Confirmed	Details	
	On Demand	02/03/2020 01:21:54 PM	02/03/2020 03:53:24 PM	Incomplete	0	Not Confirmed	Details	
	On Demand	02/03/2020 12:58:02 PM	02/03/2020 12:58:02 PM	Image not Matched	0	Confirmed	Details	
	On Demand	02/02/2020 10:52:44 AM	02/03/2020 12:19:10 PM	Incomplete	0	Not Confirmed	Details	
	Random	02/03/2020 11:41:28 AM	02/03/2020 12:01:40 PM	Incomplete	0	Not Confirmed	Details	
	Random	02/03/2020 11:51:27 AM	02/03/2020 11:51:27 AM	Incomplete	0	Not Confirmed	Details	
	Fixed	02/03/2020 09:05:02 AM	02/03/2020 09:35:50 AM	Enrollee Missed Test	0	Not Confirmed	Details	

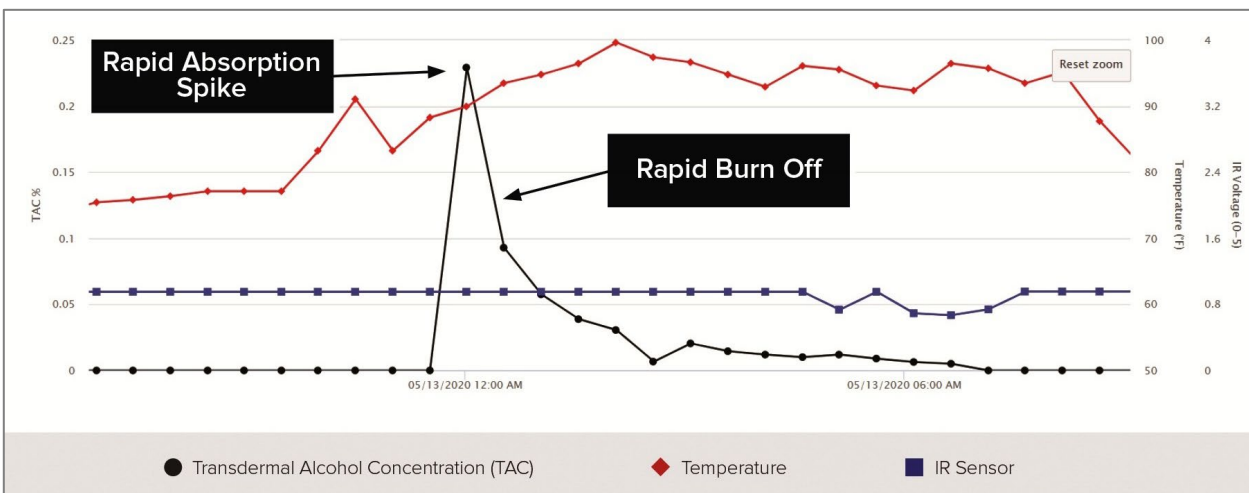
How SCRAM Connects



Confirmed Alcohol Consumption



Environmental Alcohol Detection



11. Attach the Service Level Agreement for the Alcohol Monitoring product(s) you are proposing.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus works with each customer to develop an acceptable Service Level Agreement based on the requirements defined.

Additional performance metrics are tracking for internal review and improvement and will be available to the Participating Entity on a schedule agreed upon by both parties. Securus Monitoring already collects the following metrics:

- **Number of Product and/or Service** malfunctions per day, week, and month, along with descriptions of nature and cause of malfunctions and associated plans to avoid future errors. This information is collected by our manufacturing team and reviewed on a weekly basis to highlight areas of possible improvement.
- **Speed of proposer's resolution of** malfunctions, errors, or other Product and Service maintenance requests. This information is collected from Salesforce.com and available to the Participating Entity.
- **Frequency of regular servicing and** upkeep maintenance for devices, and adherence to any maintenance plan created by Participating Entities and proposer. We have agencies that proactively clean and inspect devices and Securus Monitoring provides a report of device age to assist with this process.
- **In instances where Securus** is responsible for installation of our products, a report detailing the time to install and compliance with the court-ordered schedule.

Since each Participating Entity may require specific reporting deadlines, Securus will work with each agency to ensure compliance expectations are met.

Every calendar quarter, Securus sends a survey to all customers requesting information about our products and services. These surveys include questions regarding our Customer Success Manager performance, software performance, device performance, training services and materials, technical support services and Monitoring Center services. Additional questions can be added at the Participating Entity's request.

Securus is also open to additional government evaluations and specific forms that may need to be completed on a regular basis. We will work with the Participating Entity on these forms and submission requirements.

SCRAM

SCRAM also works with each customer to develop an acceptable Service Level Agreement based on the requirements defined.

ALL QUESTIONS BELOW MUST BE ANSWERED REGARDLESS OF THE CATEGORY(IES) TO WHICH YOU ARE RESPONDING.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

D. CUSTOMER SATISFACTION.

1. Provide evidence of your customers' satisfaction with your product or services.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus conducts **annual customer satisfaction surveys** with all active customers to assess overall performance and service quality. In **January 2026**, customers were asked to respond to a standardized set of questions evaluating their overall experience with **Securus**.

Based on survey responses received, **Securus achieved an average overall satisfaction rating of 4.1 out of 5 stars**. These results are consistent with the Company's **strong customer retention rates** and are further supported by **long-standing customer relationships and available references**.

Sample survey questions and additional details regarding the survey methodology can be provided **upon request**.

a. Client retention rate during the past 3 years

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus has the following client retention rate for the past 3 years for electronic monitoring:

Electronic Monitoring Client Retention Rate

Year	Retention Rate
2025	97%
2024	96%
2023	88%
Average 3-year retention rate	94%

b. Customer surveys/references

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

**Customer Name: California Department of Corrections and Rehabilitation (CDCR)
Division of Adult Parole Operations (DAPO)**

Contact Name:	Wendy Enos	Title:	Chief Deputy Administrator
Address:		Telephone/Fax:	(916) 709-6132

	9838 Old Placerville Rd Sacramento, CA 95827	Email:	wendy.enos@cdcr.ca.gov
Enrollees:	9,271	Products Implemented:	BLUtag, BLUhome, BLUbox, BLUband, BLUscan, BLUtwo.

**Customer Name: California Department of Corrections and Rehabilitation (CDCR)
Division of Adult Parole Operations (DAPO)**

Contact Name:	Aimee Sugapong	Title:	Parole Administrator
Address:	9838 Old Placerville Rd Sacramento, CA 95827	Telephone/Fax:	(916) 813-5527
		Email:	aimee.sugapong@cdcr.ca.gov
Enrollees:	9,271	Products Implemented:	BLUtag, BLUhome, BLUbox, BLUband, BLUscan, BLUtwo.

**Customer Name: California Department of Corrections and Rehabilitation (CDCR)
Division of Adult Parole Operations (DAPO)**

Contact Name:	Victoria Quinones	Title:	Staff Service Manager I
Address:	9838 Old Placerville Rd Sacramento, CA 95827	Telephone/Fax:	(530) 217-7350
		Email:	victoria.quinones@cdcr.ca.gov
Enrollees:	9,271	Products Implemented:	BLUtag, BLUhome, BLUbox, BLUband, BLUscan, BLUtwo.

Customer Name: Los Angeles County Probation/LA Pretrial Services

Contact Name:	Curtisa Taylor	Title:	Lead Senior Investigator
Address:	9150 Imperial Hwy Downey, CA 90242	Telephone/Fax:	(323) 803-3749
		Email:	curtisa.taylor@probation.lacounty.gov
Enrollees:	2,861	Products Implemented:	BLUtag, SCRAM, SoberTrack

Customer Name: Arkansas Community Corrections

Contact Name:	Jarrod Self	Title:	EM Program Manager
Address:	1302 Pike Avenue, Suite B North Little Rock, AR 72114	Telephone/Fax:	(501) 414-4851
		Email:	jarrod.self@doc.arkansas.gov
Enrollees:	458	Products Implemented:	BLUtag

c. Vendor performance ratings**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Vendor performance ratings for Securus are determined by Participating Entities through contract-specific Service Level Agreements, performance metrics, and applicable government vendor performance tracking systems, rather than through contractor-issued ratings.

2. Provide a brief history of your company.**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus Monitoring (Securus), a Satellite Tracking of People LLC (STOP) company, created in December 2004 in the State of Delaware, has helped to revolutionize the electronic monitoring industry with our pioneering one-piece GPS monitoring device, BLUtag. For almost 20 years, BLUtag and VeriTracks, our secure, web-based monitoring platform, have provided more than 900 Federal, state, county, and municipal agencies unparalleled service in support of their community supervision programs.

Since its inception, Securus distinguished itself among electronic monitoring providers through technology innovation and unmatched responsiveness to customers. From the beginning, we have referred to our customer agencies as “partners,” reflecting the imperative we must first understand their program and operations and then adapt our technologies to meet their needs, rather than attempting to sell a “one-size-fits-all” solution. We designed our organization to allow the key leaders of software, hardware, and customer operations (some of whom have been with the company since the beginning) to remain close to daily operations, even as our customer base has grown.

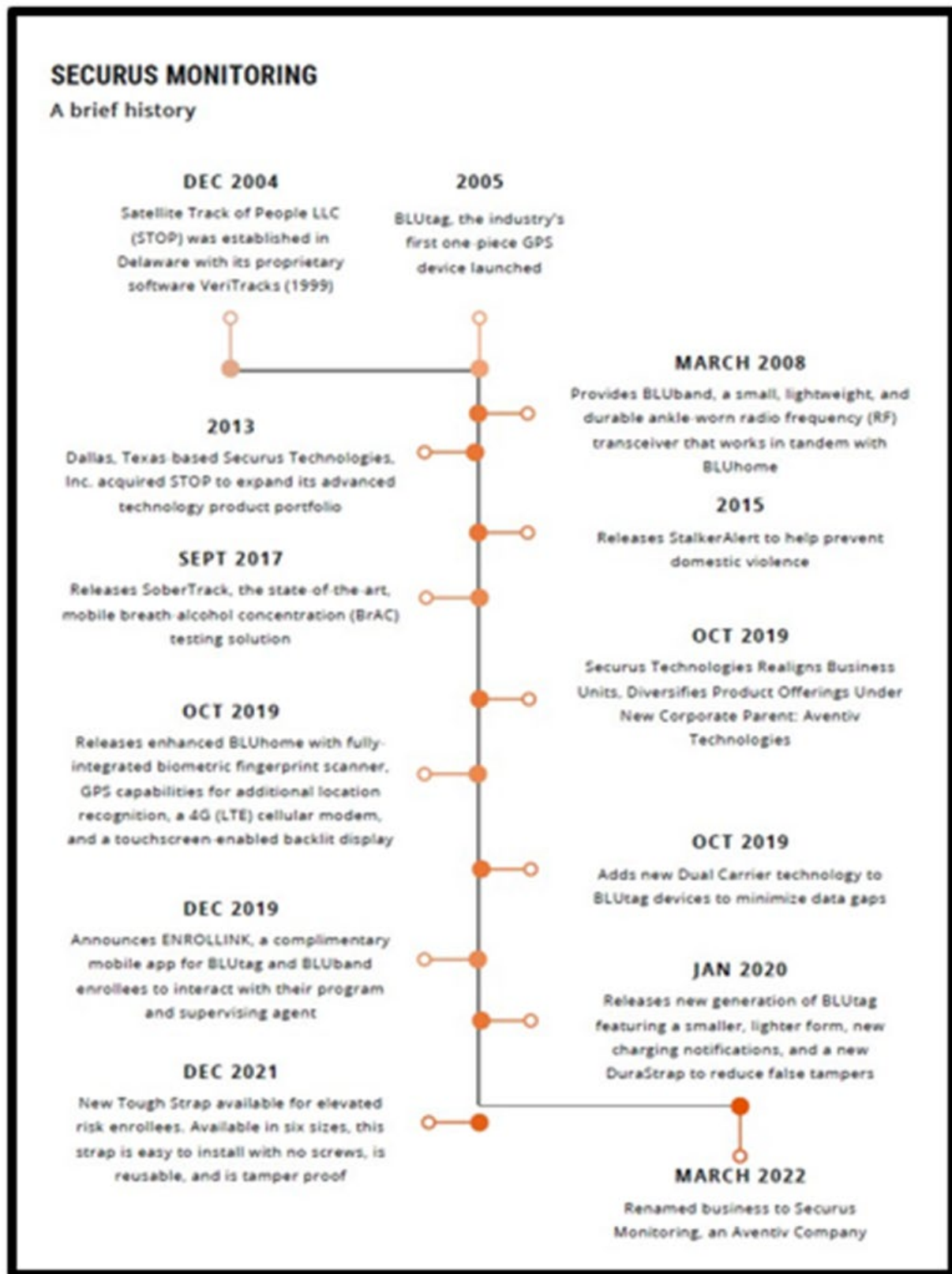
In December 2013, Dallas, Texas-based Securus Technologies, Inc. acquired STOP as part of the strategy to expand its advanced technology product portfolio. Securus is the unquestioned technology leader in the law enforcement, corrections, and public safety industries with more technology patents issued and pending than all its competitors combined. While Securus continues to operate as a wholly owned, independent subsidiary, cooperation with other Securus subsidiaries has accelerated Securus' product development and innovation in areas such as mobile applications and advanced data analytics.

Securus Technologies' purchase of STOP brought a new level of financial stability and significant investment. Over the past eighteen months, Securus has increased staff by more than twenty-five percent to nearly 140 associates. Additionally, Securus has invested millions of dollars in platform technology upgrades, increasing data processing capabilities more than 100-fold while maintaining fully redundant, Tier IV Data Centers. New investments have also enhanced the functionality of both our hardware and software to meet the evolving needs of our customers.

In 2017, we reorganized our customer-facing departments to streamline customer interactions and provide backup to all customer-facing employees. We also invested in an industry-leading, end-to-end Customer Relationship Management platform, so every Securus employee has access to account history, and our responsiveness can be documented, measured, and consistently improved.

SECURUS MONITORING

A brief history



3. Describe your company's growth during the past three years.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus continues to grow year after year, and we are excited to share our growth initiatives:

Goals and Purposes

Since 2004, Securus has been revolutionizing the EM industry with our patented one-piece Global Positioning System (GPS) monitoring device, BLUtag. Securus has long been an industry leader, providing electronic monitoring solutions to law enforcement agencies around the world for nearly two decades. Our hard-earned position at the top of a competitive EM market is the result of a singular pursuit: To assist our law enforcement and community corrections partners in creating better outcomes for the communities they serve and the offenders they supervise. Using this approach, each of our products and services have been specifically developed to support effective community supervision and enhance public safety. Below are three of the highest priorities Securus has identified which we believe will help the Participating Entity to continue its model of excellence in the field of community corrections:

Innovative Products

Our longevity and success come from our ability to differentiate ourselves through the creation of true technological innovation—not imitation—and the sound and effective application of those innovations which help our customers overcome the ever-changing challenges. As proof of our innovation, we have been awarded 29 patents—and counting—for our electronic monitoring solutions. Securus continues to enhance its hardware, software, and monitoring system platform to stay ahead of the evolving trends in community corrections. With this commitment to providing the best products and support in the market, Securus is positive it can continue to meet the Participating Entity's needs today, and we are committed to evolving with your agency in the future.

Understanding Our Customers' Needs

As the first company in history to offer a one-piece GPS device, Securus has always been a pioneer of innovation in the EM world. However, we have never settled for the status quo and have continued to evolve our products and services by closely partnering with each agency to understand new trends, challenges, and goals. Our strategy has been to understand both the technical needs and the operational needs as we continue to develop new products and services. Our close connection with agency leaders and staff has resulted in never-ending product improvements designed to create greater efficiencies while also providing better data for more informed supervision decisions.

Unmatched Responsiveness and Service

Through our close working relationships with our customers, we continue to go back to the adage: “The customer is always right!” As a result, we pride ourselves on our ability to listen well and respond quickly and effectively to our customers’ needs. Over the years, Securus has made many customized changes to hardware and software applications based on challenges being experienced by our customers. Below are just a few:

Informatics (Data Analysis)	Visits (Data Analysis)
Areas of Interest (Zones)	Wi-Fi (Tracking)
Dual Carrier (Cellular Capabilities)	BLUhome4 (Receiver)
ENROLLINK (Offender Application)	Associations (Data Analysis)
VeriTracks Mobile (Officer Application)	Entire Caseload (MapDisplay)
Mobile Chargers (Accessories)	GPS to RF Conversion (EMDCapabilities)
Data Integration (with Offender Management Systems)	Dual Fiber OpticCables (Durability and Accurate Reporting)

We know that in a moment’s notice, supervising agencies will be presented with a new problem or challenge. As we have demonstrated time and time again, Securus is committed to quickly responding to any problem or need the Participating might experience and developing a solution to overcome it.

Vision for the Future

In the same way the Participating Entity delivers the highest level of community supervision, Securus does the same in the EM industry. We lead by focusing on the small details of our products and services while also focusing on your agency’s over-arching goals. As we continue to evolve as a company, you can rest assured that any adjustment we make will fit into our shared goals of improving public safety, creating efficiencies for our customers, and improving outcomes for supervised offenders.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus, an Aventiv/Satellite Tracking of People LLC company, has been developing and marketing our GPS technologies for over 20 years. Since early 2005, we have provided

government agencies and independent service providers with a proven and reliable electronic monitoring system and a variety of services for supervising offenders in the community. The original BLUtag® was introduced in 2004, BLUhome® (home-based receiver) was introduced in 2006, and BLUband® in 2008. Updates and improvements are continuously being made to our products to keep up with emerging Agency and community safety needs.

To date, we have contracted with more than 900 government agencies and independent service providers in 46 states, including the District of Columbia, that use our monitoring system to supervise adult and juvenile offenders in the community.

With a rich history of innovation that focuses on Agency needs, Securus is a knowledgeable, resourceful, and responsive solution provider for these government agencies, as well as many others across the country.

Since its inception, Securus has distinguished itself among electronic monitoring providers through technology innovation and unmatched responsiveness to customers. As evidence of our positive working relationships, we refer to our customer agencies as “partners,” reflecting the imperative we must first understand their program and operations and then adapt our technologies to meet their needs, rather than attempting to sell a “one-size-fits-all” solution. We designed our organization to allow the key leaders of software, hardware, and customer operations (some of whom have been with the company since the beginning) to remain close to daily operations, even as our customer base has grown.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus uses VeriTracks Application Program Interfaces (APIs) for database integration with other customers. We have created single enrollment capability between our customers’ state offender management systems (SOMS) and VeriTracks. This data integration process allows for the seamless transition of key mapping fields in SOMS to correspond with data fields in VeriTracks to auto-populate, eliminating the need for agents to enter the same data into two systems. The integration is customizable to incorporate any new necessary data and can be transferred in either direction.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is in the process of implementing advanced machine learning into VeriTracks and our enrollee smartphone application, ENROLLINK. This analysis will include notifications to the enrollee to assist with ensuring that they are in compliance with their conditions of supervision and successful with reintegration. We will also be implementing a RAG flow chatbot into VeriTracks to help with FAQs, workflows, and automated reporting.

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?

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

While many of our product components are assembled in the USA and sourced domestically, there are a few that are procured from China and Korea.

Specifically, the batteries used in our products are sourced from two (2) vendors in China and Korea and our straps are manufactured in China. The batteries we use are commercial off-the-shelf (COTS) products and can be sourced from multiple vendors outside of our current sources. We have never had an instance where we were unable to obtain a supply of batteries for our devices. However, in an abundance of caution, we procure batteries in bulk, usually in orders of 10,000 pieces.

Our straps are sourced from two (2) vendors in China. We have maintained a relationship of over 15 years with these vendors, while changing the design and production of our straps multiple times. Securus also sources the fiber optic cable separate from our strap manufacturers to ensure the highest quality available. This fiber is provided to our strap vendors for installation into our custom product at our specifications. We order straps in bulk, with most orders being over 20,000 individual straps.

SCRAM

SCRAM Systems operates as the **original equipment manufacturer (OEM)** for SCRAM monitoring devices and **constructs, assembles, tests, and quality assures all equipment in-house**, maintaining full control over the supply chain and inventory. Equipment is **manufactured and assembled in the United States** and shipped from **U.S.-based SCRAM Systems facilities**, allowing the company to maintain sufficient on-hand inventory to meet program needs without extended procurement delays. As a result, **lead time to acquire equipment is minimal**, with orders placed before 3:00 p.m. Mountain Time typically **shipping the same business day** using standard delivery, and expedited or

overnight shipping available when needed. This vertically integrated, domestic supply chain eliminates reliance on overseas manufacturing and reduces risk of supply disruption.

H. Quality Assurance and Hardware Returns.

1. What are your quality assurance measures and how are they handled in your organization?

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus maintains a formal **Quality Assurance (QA) and Continuous Improvement Program** designed to ensure consistent performance, reliability, and compliance across its electronic monitoring products, software, and services. This program applies standardized controls to prevent avoidable errors, proactively identify issues, and minimize disruption to customer operations.

Securus is the original manufacturer of its proposed FCC-certified equipment, and its manufacturing facility in Houston, Texas is ISO 9001:2015 certified. The organization continually maintains and audits its quality management systems to meet this standard, with certification renewals conducted through independent audits.

Securus's QA program is organized into three integrated control areas:

1. Product Controls

Product Controls ensure that hardware and software perform in accordance with customer and contractual requirements. These controls include:

- Testing of new, refurbished, and returned equipment prior to deployment
- Software exception reporting related to alerts, data accuracy, and system behavior
- Formal testing of devices and reporting functionality before shipment

Returned equipment is disinfected, disassembled, repaired as needed, and subjected to a comprehensive series of functional tests before returning to inventory.

2. Operational Controls

Operational Controls focus on ensuring customers can fully and effectively utilize the solution. These controls include:

- Monitoring and issue intake through the Securus Solutions Center
- Capture of customer observations and user feedback through support interactions and user group meetings
- Tracking and resolution of issues within issue-tracking software

Identified performance and functionality improvements are prioritized and incorporated into regular quarterly software releases and periodic system upgrades.

3. Infrastructure Controls

Infrastructure Controls ensure that the underlying systems and platforms remain reliable, secure, and available. These controls include:

- Continuous monitoring of data centers, systems, and network components through the Network Operations Center (NOC)
- Redundant systems and geographically diverse data centers to protect against data loss and service interruption
- Proactive analysis of system performance metrics to identify and mitigate potential issues before service is impacted

These controls support high availability and system stability for monitoring and reporting services.

Ongoing Oversight and Continuous Improvement

Quality assurance at Securus is an ongoing, organization-wide responsibility. QA findings, customer feedback, and system performance data are reviewed regularly by technical, operational, and support teams. Improvements are implemented through structured change management processes and incorporated into scheduled software updates, hardware refinements, and operational enhancements.

Securus's quality assurance program combines ISO-certified manufacturing, structured product, operational, and infrastructure controls, and continuous monitoring and improvement to ensure reliable, compliant, and high-quality electronic monitoring services.

SCRAM

SCRAM Systems maintains integrated quality assurance measures across its **hardware, software, and monitoring operations** to support accurate, reliable alcohol monitoring services. Quality assurance is embedded in daily operations through the use of **centralized, web-based software (SCRAM Optix™)**, where monitoring data, alerts, and event histories are securely collected, processed, and maintained.

SCRAM utilizes **standardized monitoring and alert-handling protocols**, as defined in its Service Level Agreements (SLAs), to ensure consistent receipt, documentation, escalation,

and resolution of alerts. Monitoring Center activities are logged within SCRAM systems, creating auditable records that support accountability and program oversight.

Role-based system access controls, audit trails, and reporting tools help protect data integrity and allow authorized users to review historical records for court, compliance, and chain-of-custody purposes. Additionally, SCRAM's alcohol monitoring devices generate system alerts related to device status, tamper events, and communication issues, enabling early identification of potential problems and timely response by supervising agencies.

Through centralized data management, standardized procedures, and secure system controls, SCRAM Systems' quality assurance practices support consistent service delivery and reliable monitoring outcomes.

2. Describe your return policy for hardware.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus provides a **"no questions asked" hardware return policy** for SoberTrack devices throughout the contract term. When a device requires return for malfunction, maintenance, calibration, or replacement, the Participating Entity contacts the Securus Solutions Center to initiate the process, and a **prepaid return shipping label** is provided. Returned devices are inspected and tested upon receipt, and units not meeting performance standards are **repaired or replaced with new or like new equipment** under a **lifetime warranty against manufacturer defects**. VeriTracks proactively tracks calibration thresholds, allowing **advance replacement** so agencies can return devices without interruption to monitoring services.

Before we ship equipment, each device must pass rigorous and comprehensive testing to ensure its functionality and reliability. We certify that all proposed equipment is operable, free from defect or damage and operational prior to shipping. The Participating Entity can reject inoperable or unacceptable equipment and return it for replacement equipment.

We provide a lifetime warranty against malfunction if the Product User does not abuse, damage, or neglect the equipment. We also have a no-questions-asked return policy on all proposed equipment, which allows the Participating Entity to return any piece of equipment at any time for any reason.

All Securus equipment contains a bar code for tracking. When a device is returned/shipped, the bar code is scanned and recorded into our Repair Log system. This system contains all inventory, maintenance and service records for each piece of equipment, including test records used to certify the device such as GPS, Shock, Water, Tamper, and Battery Life. It is tied to our manufacturing and accounting system, and through a proprietary process, our monitoring software, VeriTracks.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
Date	UICP S/N	Quantity	Functional	Connect	Battery	Cell strength	GPS Radius	GPS	GPS skip points	Disposition	Tag location	TEST SUMMARY	K/S	%	NOTES				
08/19/21	22-021454	1		P	NC					no charge		stock	851	36.88%	• Stock- if all passes				
08/20/21	22-021790	1	Pass	P	P	P	26	P	P	stock		troubleshoot	152	23.27%	• No charge- if battery does not charge				
08/20/21	22-021813	1	Fail	P	P	P	0	P	P	troubleshoot		cut-open & refurb	254	83.64%	• Cut-open & Refurb- functional pass, Battery fail, Cosmetic fail				
08/20/21	22-021875	1	Fail	P	P	P	0	P	P	troubleshoot		no charge	38	4.61%	• Troubleshoot- cosmetic pass, battery pass, functional fail				
08/20/21	22-021477	1	Fail	P	P	P	0	P	P	troubleshoot			595	72.12%					
08/20/21	22-021930	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021948	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021963	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021934	1		P	NC					no charge									
08/20/21	22-021931	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021933	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021947	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021906	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021927	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021942	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021920	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021923	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021929	1	Fail	P	P	P	0	P	P	troubleshoot									
08/20/21	22-021947	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021948	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021955	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021950	1	Pass	P	P	P	26	P	P	stock									
08/20/21	22-021790	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021979	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021936	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021937	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021937	1	Pass	P	P	P	26	P	P	cut-open & refurb									
08/20/21	22-021937	1	Pass	P	P	P	26	P	P	cut-open & refurb									

tag missing



SCRAM

SCRAM Systems maintains a **formal Return Merchandise Authorization (RMA) process** for the return, repair, replacement, and scheduled maintenance of SCRAM hardware.

Return Authorization (RMA) Process

When a device requires repair, replacement, or scheduled maintenance, the Participating Entity contacts **SCRAM Systems Customer Service or their assigned Account Manager** to request a Return Merchandise Authorization (RMA). SCRAM Systems performs initial troubleshooting to determine whether the issue can be resolved remotely or if the device should be returned.

Once an RMA is issued, SCRAM Systems provides a **prepaid shipping label** and return instructions. Returned devices are tracked by RMA number upon receipt to ensure proper handling and documentation.

Repairs, Maintenance, and Replacement

SCRAM Systems is responsible for **equipment maintenance, repair, and recalibration** for SCRAM devices under normal use and warranty. Devices returned for scheduled maintenance or malfunction are **inspected, tested, and repaired or replaced with new or "like new" equipment** as appropriate.

For devices requiring recalibration (e.g., SCRAM CAM®), SCRAM Systems issues a **scheduled maintenance RMA** at the appropriate interval and coordinates the return at no cost to the Participating Entity.

Shipping Responsibilities

SCRAM Systems **covers standard shipping costs** associated with returning and replacing hardware for repairs, maintenance, or warranty issues. Replacement devices are typically shipped promptly to minimize program disruption, with expedited shipping available when required.

Warranty and Condition

All SCRAM hardware is **thoroughly tested prior to shipment**, provided under warranty, and maintained in proper working order throughout the contract term. Equipment upgrades and replacements due to normal wear or manufacturer defect are provided in accordance with contract terms

I. Implementation and Promotion of the NASPO ValuePoint Master Agreement.

1. Describe your company's experience working with contracting cooperatives.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is familiar with contracting through purchasing cooperatives and understands the unique requirements, governance models, and compliance expectations associated with these vehicles. We have been participating in this current NASPO contract since 2013. Contracting cooperatives are designed to streamline procurement while maintaining competitive, transparent, and legally compliant sourcing processes, and we align our proposal, pricing, and contract administration practices accordingly.

When working with cooperative contracts, our approach emphasizes:

- **Compliance with lead-agency solicitation terms**, including pricing structures, reporting, and audit requirements
- **Consistency across participating members**, ensuring equitable access to contract terms and services
- **Efficient onboarding and implementation**, recognizing that cooperatives often serve multiple agencies with varying operational needs
- **Clear communication and contract stewardship**, supporting both the cooperative administrator and participating entities throughout the contract lifecycle

Where applicable, we support cooperative contracts by leveraging standardized processes, scalable service delivery models, and dedicated contract management resources to ensure participating agencies receive the full value of the cooperative agreement.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus has one cooperative contract – NASPO ValuePoint Cooperative with 46 current customers, annual sales volume of \$2,421,795 (2025), NASPO does not exceed pricing for products.

3. Describe how you intend to market your Master Agreement and encourage participation among potential Participating Entities, including state governments.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

As one of the vendors that has utilized the NASPO contracting vehicle with the highest participation under the portfolio, Securus understands the importance of promoting the use of the Master Agreement. We appreciate the value of leveraging the expertise and buying power of the many states and other participating entities.

The benefits of using the Master Agreement are immense as it provides:



As one of the largest providers of technology, serving 3,400+ correctional facilities we have a percentage of current customers not utilizing NASPO. There is an exciting opportunity to convert existing customers to the NASPO contract. Securus will market the agreement to state Chief Procurement Officers (CPOs), staffers, potential agencies, and political subdivisions.

All our Account Executives have received extensive training on the Master Agreement, along with annual custom refresher courses, so they can educate and promote the agreement in their interactions with procurement departments. All Securus associates who interact with potential agencies understand the benefits of a cooperative agreement and how an entity can qualify to buy from the agreement and help agencies feel more comfortable with the use of the NASPO ValuePoint Master Agreement.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus has launched a dedicated web site promoting the contract at <https://securustechnologies.tech/naspo>.

The website explains the Master Agreement and its benefits, providing links to crucial documents, such as the Securus Model PA, Master Agreement, Amendments and Pricing Documents. Securus has also created and developed a library of customer information and promotional materials, as well as FAQs on the website.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus has appointed Rachel Drew as our dedicated NASPO program manager, dedicated to promoting and coordinating all aspects of NASPO-related activity for Securus. Rachel has attended the in person NASPO training given in Austin, TX with Bart Lemmon. She maintains Securus' registration on the NASPO ValuePoint's Supplier Portal and is well versed in the "Supplier Academy" and written materials found here.

For over 5 years Securus has sent a team to The Exchange annual conference sponsored by NASPO and is registered for this year upcoming in April. We value the time to talk to CPOs at this conference and believe participation is important to the promotion of the Master Agreement.

Securus has and will continue to:

- Create custom handouts that promote the agreement and can be provided to state agencies when making Sales contacts, visits, and National Industry Tradeshows
- Market the contract through an aggressive aggregated pricing custom model

- Utilize NASPO resources when agencies are unsure of legalities, and
- Provide factual letters of reference from participating agencies

Securus allocates dedicated **contract administration, account management, legal, sales, and operational resources** to support the effective administration of the Master Agreement and Participating Addenda. These resources are responsible for contract compliance, coordination with Participating Entities, reporting, onboarding support, and ongoing contract stewardship in accordance with NASPO ValuePoint requirements.

Securus assigns **contract administrators and program management personnel** to oversee Master Agreement obligations, including adherence to contract terms, pricing, reporting, and administrative fee requirements. Account management and customer success resources support Participating Entities throughout onboarding, implementation, and ongoing utilization of the agreement. Legal and administrative staff are available to support Participating Addendum execution and address entity-specific requirements.

Training for Internal Staff

In alignment with NASPO ValuePoint requirements, Securus provides targeted education and training to its contract administrators and sales/marketing workforce regarding:

- The scope and terms of the Master Agreement
- Participating Addendum processes
- Eligible Participating and Purchasing Entity use
- Compliance with Master Agreement pricing and administrative requirements

This training is designed to ensure staff understand the competitive nature of NASPO ValuePoint procurements and consistently represent contract terms and pricing accurately and compliantly.

Ongoing Oversight and Compliance

Securus supports continued staff familiarity and compliance through ongoing internal coordination, updates to contract documentation, and participation in annual contract performance reviews with the Lead State and NASPO ValuePoint. These reviews may include discussion of training effectiveness, reporting accuracy, marketing practices, and adherence to Master Agreement requirements.

Securus assigns dedicated contract, account management, legal, and administrative resources to its Master Agreements and provides structured training to ensure staff understand and comply with NASPO ValuePoint terms, pricing, and participation requirements.

6. Describe how you intend to encourage adoption and usage of your Master Agreement by Participating and Purchasing Entities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus will encourage adoption and usage of the Master Agreement by Participating and Purchasing Entities through proactive outreach, education, and responsive support focused on ease of participation and ordering. Our approach emphasizes clear communication of contract scope, pricing, and benefits available through execution of a Participating Addendum, supported by readily accessible contract documentation and designated points of contact. We will work directly with procurement officials and authorized users to facilitate efficient onboarding, address entity specific requirements, and ensure agencies understand how to utilize the Master Agreement in compliance with applicable procurement policies. Ongoing engagement and contract stewardship will be provided to promote continued usage and maximize the value of the Master Agreement.

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?)

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus's approach to negotiation of Participating Addenda is collaborative, efficient, and focused on timely execution while maintaining consistency with the Master Agreement. We recognize that Participating Entities may require entity specific terms and conditions to address statutory, regulatory, or operational requirements, and we are flexible in incorporating such language into Participating Addenda, provided it does not conflict with the Master Agreement. Where applicable, we request that Participating Entities identify statutory or regulatory citations supporting entity specific requirements to facilitate efficient review and approval. Securus will devote appropriate legal, contract, and business resources to support the simultaneous negotiation of multiple Participating Addenda and will work directly with each Participating Entity to reach mutually acceptable terms that comply with applicable procurement authority and policies.

8. Describe your ability to provide products and services immediately upon execution of a Master Agreement and Participating Addenda.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is prepared to provide products and services immediately upon execution of the Master Agreement and applicable Participating Addenda. Securus is the OEM for SoberTrack, this allows us to effectively support timely deployment. Our internal processes

are structured to support prompt activation following contract execution, including assignment of appropriate contract management and customer support resources and coordination with Participating Entities to confirm ordering, invoicing, and implementation requirements. Once a Participating Addendum is fully executed, Securus can accept orders and begin performance in accordance with the terms of the Master Agreement and the Participating Entity's specific requirements, ensuring a timely and compliant transition to service.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus will ensure that summary and detailed sales information is promptly, completely, and accurately reported by its dealers, partners, and resellers through contractually required reporting obligations and centralized oversight. Securus will require all sales made under the Master Agreement and applicable Participating Addenda to be captured and reported in accordance with NASPO ValuePoint reporting requirements. Sales data will be reviewed and validated prior to aggregation to support accurate quarterly submission of Summary Sales Data and Detailed Sales Data using the reporting format, tool, or template prescribed by NASPO ValuePoint. Timely and complete reporting of sales data will be treated as a material requirement of the Master Agreement to ensure full compliance with NASPO ValuePoint administrative fee and reporting obligations.

SCOPE OF WORK

This Scope of Work describes the Deliverables being sought through this Request for Proposal (RFP) and the scope of what Contractors are expected to offer through a Master Agreement resulting from this RFP. The Scope of Work is intended to provide potential Offerors with sufficient basic information to submit a proposal. It is not intended to limit a proposal's content or exclude any relevant or essential data.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

I. BACKGROUND AND DEFINITIONS

A. Overview: The State of Nevada with NASPO, is soliciting proposals from qualified Contractors to provide comprehensive electronic monitoring solutions and related services for individuals under supervision. The RFP includes but is not limited to, Global Positioning System (GPS) Monitoring, Radio Frequency Monitoring (RFM), and Alcohol Monitoring (AM). Hardware, software, installation, maintenance, and support of the equipment are also included as part of the Scope of Work. The intent is to establish multiple contracts with reliable, secure, and cost-effective Contractors that promote compliance with Participating Entity supervision conditions and the successful management of monitored individuals.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

B. 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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus meets or exceeds the requirements outlined in the National Institute of Justice, Standard Offender Tracking Systems, 1004.00. All equipment provided is in new, or certified like-new, condition and passes rigorous testing prior to shipment. This testing includes thorough cleaning as well as an external inspection for defects or damage. Each monitoring device must pass a water test to confirm the device is waterproof and the internal diagnostic testing of each piece of equipment confirms all technological components are in working order.

Securus (STOP) FCC Certificates

All Securus equipment is designed to be rugged, durable, and meet the highest level of performance while being FCC certified. If the State would like a copy of the SoberTrack certificate, they can be provided upon request.

EQUIPMENT	DIMENSIONS AND WEIGHT	FCC#	DESCRIPTION
BLUtag (GPS)	2.5" x 2.5" x 1.24" 5.7 ounces	S5EBTV81018	FCC-certified one-piece active Global Positioning System (GPS) monitoring device coupled with VeriTracks, web-based tracking application. Works with BLUhome or BLUbox.
BLUbox	4.25" x 3" x 2.25" 7 ounces	S5EAA90548	FCC-certified home receiver unit that works with BLUtag to confirm when the client is at home
BLUhome	8" x 7" x 2.5" 10 ounces	S5EBH0107A	FCC-certified home receiver unit that reports monitoring data to VeriTracks using nationwide cellular service or (as an option) the digital/landline phone service in the client's home

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TUV Rheinland of North America, Inc.
1279 Quarry Lane Suite A
Pleasanton, CA 94566

Date of Grant: 12/24/2019

Application Dated: 12/23/2019

Satellite Tracking of People LLC
5353 West Sam Houston Parkway North
Suite 190
Houston, TX 77041

Attention: Stephen Freathy , Mr

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: S5EBTV81018

Name of Grantee: Satellite Tracking of People LLC

Equipment Class: Digital Transmission System

Notes: Ankle worn electronic tracking 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>
	15C	2412.0 - 2462.0	0.078		
	15C	2402.0 - 2480.0	0.0081		
	15C	902.3 - 914.9	0.021		

Listed output power values are from conducted measurement.

The highest reported extremity (limb worn) SAR value for this radio transmitter (DTS) is 0.13
W/kg.

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

RFI Global Services Ltd
Pavilion A Ashwood Park, Ashwood Way
Basingstoke, Hampshire, RG23 8BG
United Kingdom

Date of Grant: 08/31/2006

Application Dated: 08/31/2006

Satellite Tracking of People LLC
102 Woodmont Blvd
Suite 800
Nashville, TN 37205

Attention: Stephen Freathy , Mr

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: S5EAA90548
Name of Grantee: Satellite Tracking of People LLC
Equipment Class: Part 15 Low Power Communication Device Transmitter
Notes: BLUBOX

<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	915.0 - 915.0			

TCB

GRANT OF EQUIPMENT
AUTHORIZATION
Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TCB

RFI Global Services Ltd
Pavilion A Ashwood Park, Ashwood Way
Basingstoke, Hampshire, RG23 8BG
United Kingdom

Date of Grant: 02/21/2007
Application Dated: 02/21/2007

Satellite Tracking of People LLC
102 Woodmont Blvd
Suite 800
Nashville, TN 37205

Attention: Stephen Freathy , Mr

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: S5EBH0107A
Name of Grantee: Satellite Tracking of People LLC
Equipment Class: Part 15 Low Power Communication Device Transmitter
Notes: BluHome®

Grant Notes

FCC Rule Parts
15C

Frequency
Range (MHz)
915.0 - 915.0

Output
Watts
0.00058

Frequency
Tolerance

Emission
Designator

In the event any component of the Contractor's service becomes inoperable, the Contractor must immediately notify the Participating Entity Representative(s) or designees by telephone or most expedient means available, but no later than sixty (60) minutes after service failure.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Our proposed Account Manager, or our Monitoring Center, will call the Participating Entity' Program Manager Monitoring as quickly as possible after the start date and time of any disruption that may last longer than sixty (60) minutes. Calls will be made at any time of day, 365 days a year.

C. Definitions:

Band/Strap: Used to fasten or otherwise secure the monitor to the body of the client.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Base Station: A fixed transceiver unit installed at a specific location, typically an Client's home, that communicates with a portable monitoring device (e.g., an ankle bracelet) worn by the Client.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Client: the individual under the supervision of a correctional agency who is required to wear an electronic monitoring device.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Global Position Satellite Monitoring (GPS or GPSM): An electronic monitoring program is provided through a body-attached one-piece device or a multi-device system that provides location tracking and violation via cellular data and/or voice communication to the Monitoring Center. On a scheduled (active, hybrid or passive) basis, tracking data is communicated to the Monitoring Center who then communicates violations and equipment status alerts via email, text message, and/or manual voice message to the designated Agency contact pursuant to established protocols.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Passive Tracking: records an offender's location data throughout the day but does not transmit it in real-time. The device stores movement information, which is uploaded to a monitoring center later – typically daily – via a docking station or cellular signal, providing “after the fact” tracking.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Priority Communication: Prioritized alerts during high-traffic or peak periods. Alerts may include, but not limited to, violation of critical conditions, safety threats, equipment tampering, and serious curfew violations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Radio Frequency Monitoring (RFM): Electronic monitoring service is used for home detention. Client wears a body-attached transmitter that communicates by radio frequency with a home receiver. The home receiver transmits data to the Monitoring Center by landline telephone or by cellular communication. Monitoring Center reports

curfew violations and equipment status alerts to the designated Agency contact by email, text message, and/or manual voice message pursuant to established protocols.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Receiver: Device that collects and transmits data regarding the status of the client and their movement, the health of the receiver and the attempts to cut or tamper with the band/strap. The receiver may be either a secondary device or attached to the client via an enhanced cut and tamper resistant band.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Tamper: refers to the intentional and unauthorized act of removing, cutting, destroying, altering, damaging, disabling, or otherwise interfering with monitoring equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Transmitter: a fixed transceiver unit installed at a specific location, typically an offender's home, that communicates with a portable monitoring device (e.g., an ankle bracelet) worn by the individual.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

D. New Products/Technologies: Master Agreements may be updated in the future by amendment to address product enhancements and advances in technology.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

II. GENERAL CONTRACT REQUIREMENTS. (APPLIES TO ALL CATEGORIES)

Client damage, neglect, or abuse of an installed Product and/or Service will not be covered by Contractor, and Contractor may bill the Purchasing Entity and/or Client, at a fee schedule negotiated per the Participating Entity's Participating Addendum.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Contractor must provide delivery and service continuity of all Products and Services proposed and awarded under the Master Agreement to all fifty states, as well as the District of Columbia and U.S. territories.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Contractor must comply, at all times, with Federal, State, and local laws, and those regulations required by the Participating Entity.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Contractor must use a digital chain of custody that can be used as reliable evidence in court (secure data collection, digital logs and tracking, tamper-proof storage, digital fingerprint, access control, and system integrations). When requested by a Participating Entity, Contractor must provide a staff member from their company to testify, at no additional cost.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus provides our in-house expert witness, Mr. Jeff Marino, to ensure that Securus meets a Participating Entity's potential need for legal support. Mr. Marino possesses more than 30 years of experience in GPS and RF field operations. His experience includes supervising day-to-day operations of customer programs, data analysis, technical support, training, and providing expert witness testimony for courts as needed. Prior to joining Securus, Mr. Marino served as South Region Field Operations Manager with Sentinel Offender Services, where he maintained and developed all monitoring programs in that region. He oversaw a staff of approximately 15 Account Managers, coordinating the implementation of all programs and the training of all personnel. He also worked with BI Incorporated as a Lead Field Representative and a Monitoring Specialist. He was responsible for installing, servicing, and supporting electronic monitoring equipment and services. He served as a police officer for 10 years before entering the electronic monitoring industry.

Court-Requested Reporting and Chain of Custody

Securus follows forensic evidence handling procedures in that:

- Monitoring data is captured electronically within a secure system
- Access is limited to authorized personnel
- Reports are generated directly from system-recorded data
- Reporting follows Participating Entity and court-defined procedures

Accordingly, Securus supports court use by preserving system-generated records and controlled access, while the Participating Entity remains responsible for submitting reports and satisfying jurisdiction-specific evidentiary or chain-of-custody requirements.

Securus supports court reporting requirements by securely capturing and maintaining monitoring data within its web-based platform and generating reports in accordance with Participating Entity protocols, while final evidentiary handling and chain-of-custody determinations remain subject to court and jurisdictional requirements.

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 with in 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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is AICPA SOC 2 compliant. Securus has written policies and procedures for all data and physical security, and a copy of these will be provided to Participating Entity upon request.

Securus takes a proactive approach to application and network security, upgrading security measures on a continuous basis. We use industry-leading technology and tools to provide the highest levels of security to protect monitoring data, prevent hacking into our monitoring system, and implement fast fault recovery. Our system's security model was designed by General Dynamics, and it applies the same policies and procedures as those used by the U.S. Department of Defense and U.S. intelligence agencies. VeriTracks immediately reports all attempts of unauthorized access to our 24/7 Network Operations Center, and our IT engineers can generate reports detailing the attempt(s). To date, VeriTracks has never been hacked or had a data breach.



Securus' proactive approach to system security includes using industry-standard security measures to prevent unauthorized access to the data and implement fast recovery measures.

We break our security measures down to: Application Security, Network Security, and Physical Security.

Application Security

Application security begins with access only over HTTPS followed by the username and password assigned and maintained by the application. User administrators create user accounts, and the system assigns and e-mails strong passwords. Passwords cannot be captured because VeriTracks uses Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt all traffic. Each account is created as a restricted user (with permission to view only), a normal user (with permission to create and modify data) or an administrative user (with permission to create users as well as create and modify data). Most users are created as normal users. Additionally, two-factor authentication can be utilized with VeriTracks, requiring the staff to have a username, password, and access to a telephone to receive a text message or a phone call with a unique code.

Network Security

Network security is provided by integrating state-of-the-art security system products with corresponding security best practices. The network is divided into multiple zones. The zones are designed to logically segment the network traffic, allowing specific access into and out of each zone, as necessary. All network segments are protected by high-availability and fully redundant firewalls. Only HTTPS, SCP/SFTP, and our electronic monitoring devices traffic are allowed into the network, and all SCP/SFTP traffic is restricted by source address. No traffic from the Internet is ever directly accessible to the internal segments where VeriTracks data is hosted. VeriTracks is only accessible through SSL/TLS with 256-bit

encryption to protect the information being passed through the internet and to support older versions of web browsers.

Physical Security

Our Data Centers are secured against physical intrusion by a well-known third party. They provide financial-grade protection for our mission-critical Internet operations. The centers are physically secure with on-site security officers 24 hours a day, 365 days a year. They have an array of security equipment, as well as policies and procedures to control, monitor and record who is granted access to the facility, when the individual(s) leave the facility and who was denied access to the facility. Only Securus-authorized personnel have access to the cages in the Data Centers housing the VeriTracks servers. Both Data Centers have the following physical security measures:

Digital video monitoring and recording of entrances, exits and individual cages	CCTV integration with access control and alarm system
Card key (electronic badge) and biometric (fingerprint) access controls	Mantraps at each entrance into and out of the facility
Fire detection and suppression equipment throughout the facility	Equipment checks upon arrival
Shipping and receiving area walled off from co-location areas	

Data Security

To ensure there is no loss of data should one of the chains goes offline, Oracle's DataGuard offering keeps the two VeriTracks data centers in sync. While the solution is configured in an active/standby pattern, if a disaster occurs in the primary Data Center, the standby can be brought up as an active instance, and all web and device traffic can be pointed to the redundant Data Center. During this time, no data is lost, and devices continue to collect and report monitoring data.

Our VeriTracks database uses redundant Oracle Exadata Database Machines. These are engineered systems that incorporate both a computer and storage system specifically designed to provide the best Enterprise Oracle database instances. With our production databases residing on these engineered systems, VeriTracks can take advantage of the

data's architecture where data encryption is decoupled from the database server software and is instead performed directly by the storage server hardware using stored data encryption. With this technology, both the disk and flash storage encrypt data at the point when it enters the devices, as opposed to relying on the database server software to perform the encryption.

Securus' IT Department personnel routinely test the switchover process to ensure its smooth and efficient operation. From a staffing perspective, Data Centers are managed remotely as there is no need for staff to be physically present to drive the switchover in both Data Centers. This gives Securus the benefit of true continuity with the staff executing the procedures. Where physical control of the servers is required, Data Center staff provide hands-on services.

In certain cases, this allows maintenance to be performed in a Data Center without traffic being handled (e.g., an upgrade of the firmware on VeriTracks core switch). As with any continually growing solution, updates are made to the switchover process as time progresses. Vulnerability testing is conducted quarterly by an outside auditing firm. Upon award, this schedule can be synchronized to provide the customer with results from the switchover process and include any updates and notes based on the switchover.

The exchange of monitoring information between authorized personnel and Securus personnel occurs via VeriTracks, which is only accessible to authorized users through a Hypertext Transfer Protocol Secure (HTTPS) connection. HTTPS is a combination of HTTP and the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols, which protect network traffic through 128-bit encryption.

Securus highly recommends the use of two-factor authentication for all authorized personnel. VeriTracks' standard configuration for all access is two-factor authentication provided by Google, but this can be disabled at the request of the agency.

Please see **Exhibit 1: Aventiv NIST Attestation Letter** for additional information.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Please see **Exhibit 1: Aventiv NIST Attestation Letter** for additional information.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus will contact the Purchasing Entity within 72 hours 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.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Data is not defined for this requirement. We assume that Data means the user GPS data provided by the service. Based on this assumption, Securus has read, understands and will comply.

All data centers must be based in the United States.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Our Data Centers are geographically disparate with one residing in Carrollton, Texas and the other in Atlanta, Georgia. No data is ever kept or released outside the United States.

B. Data Requirements

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The exchange of monitoring information between authorized Participating Entity personnel and Securus personnel occurs via VeriTracks, which is only accessible to authorized users through a Hypertext Transfer Protocol Secure (HTTPS) connection.

HTTPS is a combination of HTTP and the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols, which protect network traffic through 256-bit encryption.

VeriTracks also has two-factor authentication available to all Participating Entity staff to ensure access is limited to authorized users. This is provided by Google 2FA, and the agent either receives a text message or telephone call with their access code.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Application security begins with access only over HTTPS followed by the username and password assigned and maintained by the application. User administrators create user accounts, and the system assigns and e-mails strong passwords. Passwords cannot be captured because VeriTracks uses Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt all traffic. Each account is created as a restricted user (with permission to view only), a normal user (with permission to create and modify data) or an administrative user (with permission to create users as well as create and modify data). Most users are created as normal users. Additionally, two-factor authentication can be utilized with VeriTracks, requiring the staff to have a username, password, and access to a telephone to receive a text message or a phone call with a unique code.

Network Security

Network security is provided by integrating state-of-the-art security system products with corresponding security best practices. The network is divided into multiple zones. The zones are designed to logically segment the network traffic, allowing specific access into and out of each zone, as necessary. All network segments are protected by high-availability and fully redundant firewalls. Only HTTPS, SCP/SFTP, and our electronic monitoring devices traffic are allowed into the network and all SCP/SFTP traffic is restricted by source address. No traffic from the Internet is ever directly accessible to the internal segments where VeriTracks data is hosted. VeriTracks is only accessible through SSL/TLS with 256-bit encryption to protect the information being passed through the internet and to support older versions of web browsers.

Physical Security

Our Data Centers are secured against physical intrusion by a well-known third party. They provide financial-grade protection for our mission-critical Internet operations. The centers are physically secure with on-site security officers 24 hours a day, 365 days a year. They have an array of security equipment, as well as policies and procedures to control, monitor and record who is granted access to the facility, when the individual(s) leaves the facility and who was denied access to the facility. Only Securus-authorized personnel have access to the cages in the Data Centers housing the VeriTracks servers.

Securus highly recommends the use of two-factor authentication for all authorized personnel. VeriTracks' standard configuration for all access is two-factor authentication provided by Google, but this can be disabled at the request of the agency.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus follows industry-leading practices for hiring the most qualified personnel for all aspects of our company, including the maintenance, security, and integrity of our operations. We do conduct criminal background investigations on all employees prior to being hired and then randomly while employed. A copy of the results for anyone directly working on this contract can be provided at the customer's request. We do not intend to utilize any subcontractor for this contract but would apply the same criminal background investigation requirements to a subcontractor.

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. 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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.



The SCRAM Continuous Alcohol Monitoring® (SCRAM CAM®) 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.

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. SCRAM CAM:

- Encourages compliance because it eliminates testing gaps—meaning that there is no way to miss a test or drink around testing schedules.
- Uses a controlled, quantifiable sample, resulting in true continuous monitoring and the lowest false positive rate possible.
- Battery life of 90+ days significantly reduces the need for constant communication and supervision.
- 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.
- Is court-validated—meaning 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.

As the pioneer of CAM technology, SCRAM Systems launched the original Secure Continuous Remote Alcohol Monitor (SCRAM) system to the criminal justice market in 2003. In 2010, optional, built-in RF house arrest capabilities were added to the bracelet to provide dual functionality. Known today as SCRAM CAM, it is part of the SCRAM Systems line of

electronic monitoring and corrections software solutions. SCRAM CAM has monitored more clients worldwide than all other transdermal devices combined.

Equipment is at a minimum, shock, water, and tamper resistant.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

Anti-Tamper Technology

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 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 can identify proximity tampering—situations where foreign objects or barriers are placed between the bracelet and the skin to obstruct its function. These sensors continuously monitor 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.

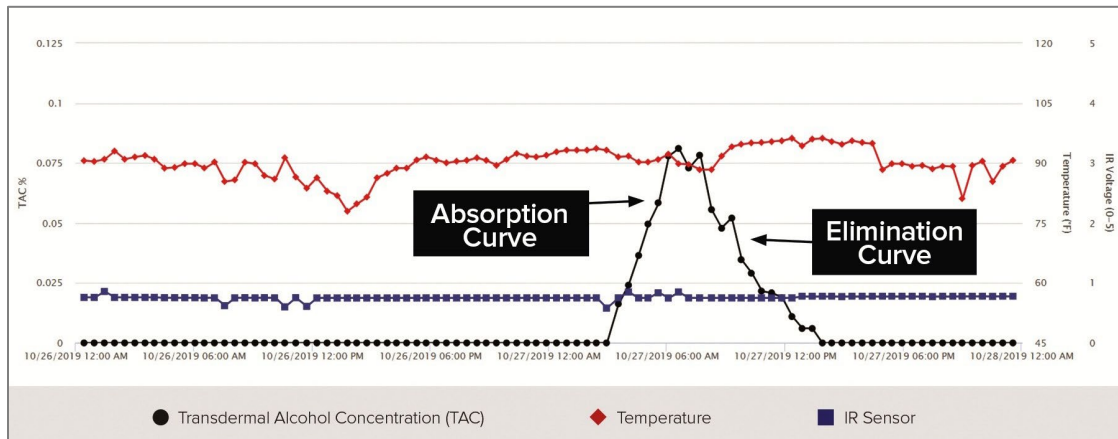
The equipment must monitor ingested alcohol in the human body using court-validated transdermal testing technology and must be able to distinguish between ingested alcohol and environmental exposure to alcohol.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM CAM distinguishes between both ingested alcohol and environmental exposure to alcohol.

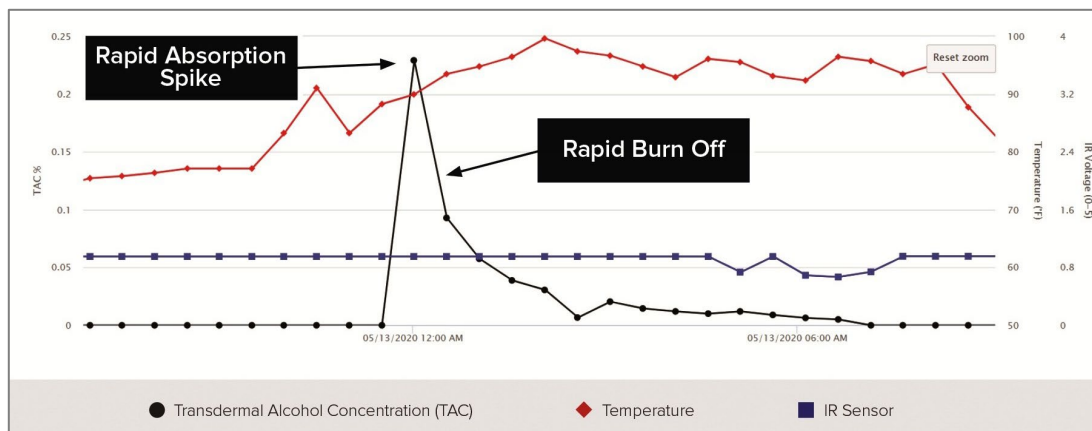
Confirmed Alcohol Consumption

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.



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.



The equipment must have a minimum of two (2) ways to communicate data to the software, such as landline, Ethernet, Wi-Fi, or cellular.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The bracelet transmits data by RF signal to the SCRAM Base Station. When data is received by the base station, it is transmitted to the monitoring software platform by telephone landline, Ethernet, Wi-Fi, or cellular communication. The software notifies the supervising authority of any alcohol alerts, tamper alerts, or equipment malfunctions so they can respond quickly to problem clients.



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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Because people excrete approximately one percent (1%) of the alcohol they drink through their sweat, if an individual has been drinking it will show up in the level of alcohol vapor present in the insensible perspiration that is constantly produced and emitted by the skin. The SCRAM CAM ankle bracelet continually collects a sample of a client's insensible perspiration and automatically tests the sample every 30 minutes, 24 hours a day. SCRAM CAM provides the industry's only true 24/7 sobriety monitoring, ensuring that authorities know conclusively if a client has been drinking or if they are compliant with the conditions of their supervision.

The SCRAM CAM device continuously collects a sample, making it easy to use with no required intervention from the client. There are no reminder calls necessary, no prompts required to initiate monitoring, and no action needed by the client to preface testing.

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 can identify proximity tampering—situations where foreign objects or barriers are placed between the bracelet and the skin to obstruct its function. These sensors continuously monitor 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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The patented SCRAM CAM bracelet is attached to the client's ankle and worn 24/7. It monitors alcohol consumption by sampling the insensible (gaseous) perspiration constantly being emitted from the body.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

Device must have demonstrated a history, highlighting the validity of the product or establishing general acceptance in the electronic monitoring community.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM® has a **longstanding, documented history of use within the electronic monitoring community** and is widely deployed by federal, state, and local justice agencies for alcohol monitoring programs. As the **pioneer of continuous alcohol monitoring**, SCRAM Systems introduced the original SCRAM CAM® technology to the criminal justice market in **2003**, with subsequent enhancements and optional RF capabilities added over time. SCRAM CAM® has been **independently tested, peer reviewed, and court validated**, and its scientific reliability has been upheld under **Daubert, Frye, and applicable evidentiary standards** in jurisdictions where challenged. This extensive operational history, combined with continued adoption by supervising agencies and ongoing product support, demonstrates **general acceptance and validity of SCRAM technology** within the electronic monitoring community.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.



The bracelet can be used as CAM-only or combined with integrated radio frequency (RF) house arrest for location monitoring. Officers can easily enable the house arrest feature through in the software at any point during a client's monitoring without the need to change equipment.

Flexible Communication.

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 software.

Range

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 Base Station includes an LED indicator and an audible alarm that can be enabled to alert the client when they are out of range.

Location Verification.

If monitoring via landline and the base station is disconnected and reconnected to an unauthorized telephone line, the SCRAM 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.

Curfew Schedules

SCRAM Optix provides an efficient means of managing curfew schedules for each client on a case-by-case basis as determined by the supervising officer(s). It enables supervising officers to easily modify any client's schedule and curfew information via flexible edit, copy, and delete features. It also allows officers to view past schedules, as well as historical change records.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix is a web-based application developed and managed by SCRAM Systems where client data is collected, analyzed, and maintained in a secure, central location. This central information hub 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.

SCRAM Optix is 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 assess detailed caseload information at-a-glance via device and status indicators.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Since mobile applications often have limited functionality, SCRAM Systems software is designed to be mobile-adaptive, allowing users to access all features available on a computer from a smartphone or tablet. It requires no additional apps and is optimized for easy viewing on any mobile device. Unlike mobile apps, which require frequent updates to maintain current information and functionality, our mobile-adaptive site ensures real-time access and performance. With client profile information at their fingertips, officers can access priority alerts such as confirmed drinking events and tampers, client addresses, and call clients right from their mobile device.

Secure login with multi-factor authentication.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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:

high atmosphere alcohol

alcohol detected report,

dual alerts (both high atmosphere and alcohol detected),
below-temperature conditions,
and prolonged high atmosphere readings

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Notification methods for all alerts include email, text, and/or a Daily Activity Plan (DAP). The DAP can be automatically delivered up to twice daily. 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.

House Arrest events can be selected as priority alerts, ensuring notification within 15 minutes of the alert either by email and/or text, as specified. Additionally, House Arrest events are integrated into the client-facing TouchPoint application, creating improved program efficiencies, and streamlining officer/client communications.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix provides a wide range of reports and graphs (using customizable fields)—from a snapshot of a single event to a comprehensive view of a client’s behavior over time all exportable in PDF, Excel, and CSV formats. These reports are customizable to best suit the Participating Entity’s needs, reducing officer workload.

Integration options with existing case management systems through APIs.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems supports integration with existing case management systems through secure, standards-based APIs. The integration framework is designed to enable **single-direction or bi-directional data exchange**, depending on the needs of the agency, and is currently in operational use with local and state monitoring programs.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix meets all applicable for FCC regulations (SCRAM CAM Bracelet: FCC ID P8M-SM0; SCRAM Base Station: FCC ID P8M-SM03) and is ISO certified. SCRAM Optix provides audit trail and data retention in compliance with CJIS security 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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix system provides role-based access controls for different user types. Unauthorized users are unable to access secure information.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix allows the Participating Entity to download data and reports from the database, through secure internet access.

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 a direct USB data transfer, or other methodology, where land line and cellular coverage is not available or is not the preferred communication method by agency personnel.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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 7500 messages).

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.

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 a week, 365 days a year.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides a **centralized and controlled monitoring center** that operates on a **24 hours per day, 7 days per week, 365 days per year basis**, staffed by trained analysts and customer support specialists dedicated exclusively to SCRAM monitoring technologies. Client data transmitted via the internet is received, analyzed, and monitored in real time, including **alcohol readings, tamper alerts, communication failures, equipment issues, and maintenance or malfunction indicators**. The monitoring center performs **continuous alert analysis and notification**, providing timely communication to agency staff through configurable alerting methods, while maintaining secure, web based access to client information through SCRAM Optix®. This structure ensures uninterrupted oversight, rapid issue identification, and consistent support for Participating Entities.

The system must include inventory tracking and management features.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix provides inventory management.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Optix will archive and retain archived data for at least seven (7) years from date the client is enrolled.

Contractor'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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The SCRAM Continuous Alcohol Monitoring® (SCRAM CAM®) system provides **automated, date- and time-stamped readings at 30-minute intervals, 24 hours per day**, by continuously collecting and testing samples of insensible perspiration. Each measurement includes **Transdermal Alcohol Concentration (TAC)** data and is accompanied by **body temperature readings and anti-tamper indicators**, allowing the system to identify and

report any attempts to obstruct, interfere with, or remove the device. Multiple integrated sensors monitor skin contact, temperature variation, and obstruction or removal attempts, and all readings and events are securely transmitted for analysis and reporting, ensuring continuous, verifiable monitoring that meets or exceeds the stated requirement.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides **automated daily summary reporting** that identifies **clients in violation of program conditions and those requiring technical maintenance**, including confirmed drinking events, tamper or obstruction alerts, communication failures, and equipment status issues. Through SCRAM Optix®, agencies may receive a **Daily Activity Plan (DAP)** delivered automatically by email and/or accessed through the secure web-based platform, with all events **date and timestamped** and reviewed by SCRAM-certified analysts prior to notification. These daily reports and real-time alerts enable supervising personnel to quickly identify required actions, prioritize responses, and maintain continuous oversight of both client compliance and equipment health.

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 time of ingestion and the Transdermal Alcohol Concentration (TAC) present in the system over the time of the event.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The SCRAM Continuous Alcohol Monitoring® (SCRAM CAM®) system provides **clear, easyto read noncompliance reports** through **SCRAM Optix®**, presenting **both graphical and numerical displays** of alcohol-related events. When alcohol is detected, reports include a **timestamped Transdermal Alcohol Concentration (TAC) curve** that graphically illustrates alcohol absorption, peak TAC, and elimination over the duration of the event, enabling agencies to **approximate the time of ingestion**. Numerical TAC values are displayed alongside the graph, and **temperature and antitamper indicators** are overlaid to distinguish confirmed drinking events from environmental exposure or obstruction attempts. These reports are generated from system recorded data, reviewed through a validated analytical process, and are accessible on demand to support enforcement actions, documentation, and court proceedings.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides **easy-to-read summary management reports** through **SCRAM Optix®**, allowing authorized agency personnel to access and generate reports related to **individual client activity, dates and duration of system use, agencywide equipment inventory status, and billing information**. Reports are available on demand via the secure, web-based platform and can be **customized and filtered** by client, date range, or program level criteria to support operational oversight and administrative review. These reports present data in a clear, organized format designed to reduce administrative burden and support program management and are **provided upon request** in accordance with Participating Entity reporting needs.

3. Customer Support and Training

The Contractor must provide a dedicated account representative.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides each Participating Entity with a **dedicated account representative** who serves as the primary point of contact for program coordination, operational support, and ongoing account management. The assigned account representative works closely with agency staff to support implementation, training coordination, reporting needs, and issue resolution, and is backed by SCRAM Systems' broader account management and services teams to ensure continuity of support throughout the contract term. This structure ensures consistent communication, accountability, and responsive service aligned with agency requirements.

The Contractor must provide support functions 24/7/365.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides **continuous support functions 24 hours per day, 7 days per week, 365 days per year** through its **fully owned and operated monitoring and support center**, staffed by trained analysts and customer support specialists dedicated exclusively to SCRAM technologies. Support services include real-time monitoring and analysis of alerts, technical assistance, equipment and communication issue resolution, reporting support, and secure access to client and program data via SCRAM Optix®. Agencies may access support at any time via phone, email, or web-based channels, ensuring uninterrupted system oversight and responsive assistance regardless of time, date, or operational need.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides **tollfree access to its customer support and monitoring center**, ensuring agencies can reach live, trained support staff at any time. The monitoring center is accessible via a **tollfree telephone number**, in addition to email and web based channels, and is staffed by SCRAM Systems personnel dedicated exclusively to 24/7/365 monitoring and support services. This ensures Participating Entities have immediate, no-cost phone access for assistance with alerts, client activity, equipment issues, and general program support.

The Contractor must provide initial start-up training that must include but not be limited to the following:

The enrollment of clients into the software system.

The installation, use, de-installation, and cleaning of the equipment.

The generation and interpretation of data/monitoring reports.

Accessing/using Contractor's technical support/help menus and monitoring center.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SCRAM Systems provides **comprehensive initial startup training at no additional cost**, delivered onsite, remotely, or via live webinar as requested, and tailored to agency workflows. Initial training includes **enrollment of clients into the SCRAM Optix® software system, hands-on instruction for the installation, use, deinstallation, and proper cleaning of SCRAM equipment, and generation and interpretation of monitoring and compliance reports**. Training also covers **accessing and using SCRAM Systems' technical support resources**, including the **Help and Support menus**, online documentation, SCRAM Systems University, and direct interaction with the **24/7/365 monitoring center**. All training materials, reference guides, and instructional resources remain available online for refresher training and new staff onboarding throughout the contract term

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

B. REMOTE ALCOHOL MONITORING (RAM)

1. Hardware

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is proud to offer SoberTrack:

Alcohol Breath Testing

SoberTrack represents the state-of-the-art mobile handheld breath alcohol testing. The device will emit an audible tone when the client needs to be tested. Additionally, VeriTracks can send the enrollee a text message as a reminder 5 minutes prior to a scheduled test and for each retest. The client acknowledges test notification through the touch screen. The device requires a deep lung blow that must be sustained for over four (4) seconds at a pressure required to access the air in the lungs. SoberTrack will alert the client during testing once it reaches the proper air pressure to assist them in conducting a successful test. During a test sequence, the advanced digital camera takes multiple images to provide for a more complete test review, eliminate blurry or partial images, and to provide image comparison to the profile image. In low light settings, the device is equipped with a LED light, which automatically turns on to assist in obtaining the best picture quality possible. Photos are processed through automated facial recognition software and, for any possible failed photograph, a comparison of the testing photo to a reference photo can be performed by the Securus Center within ten (10) minutes of the test being completed.

Another feature unique to SoberTrack is our video capture capability. Each test has a stream of video captured from the initiation of the testing sequence until the end of testing (usually 8 to 15 seconds). These video clips are stored in SoberTrack for up to one (1) week and can be downloaded by the supervising officer to provide detailed analysis of any suspect tests. These clips can be crucial in determining attempts to circumvent the testing process or having others attempt to pass a test for the client.

The completion of the test will be displayed on the touch screen display of the SoberTrack indicating if test is completed or if re-test sequences are required with the configured re-test time in minutes. If no re-test is required, the device will return to a blank screen. The device displays the status of the battery using icons when the screen is touched.

SoberTrack downloads and stores all schedules and future testing requirements. This allows it to work autonomously in alerting clients of upcoming tests even when SoberTrack



cannot find adequate cellular signal to communicate with VeriTracks. Test results, retesting data, and alert situations are stored in SoberTrack's non-volatile memory, which can store up to 10,000 events, until the information can be downloaded.

SoberTrack can perform scheduled, random, and on-demand testing on a 24/7 basis, as the device is always connected to a cellular network. Each result is deemed passing, failed due to positive alcohol/other causes, or missed. All test results are immediately sent to the customer by email and/or text message for response after confirmation/review by our automated facial recognition software. Any failed images from automated recognition are then sent to our 24/7/365 Solutions Center for a manual review of the image for a final determination of pass/fail before we alert the supervising officer.

In VeriTracks, schedules can be created to have clients perform up to 12 tests in a 24-hour period. On-demand testing can be created whenever the field officer deems necessary, on an ad hoc basis, up to 12 times in a 24-hour period as long as there are no other tests scheduled for the same time. Random testing can be set to administer up to three (3) tests during a given time frame, allowing for one (1) to four (4) hours between each test.

Device must be capable of storing test results in the RAM's memory.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack® can store test results in the device's internal memory. SoberTrack records results and associated data (including images and test history) and maintains those records until they are transmitted to **VeriTracks®**, Securus's secure Monitoring Center system.

SoberTrack maintains a testing history for each device, which is tracked and managed within VeriTracks. This confirms that test results are retained locally on the device as part of its operational workflow and then synchronized with the Monitoring Center once communication occurs.

Device must use facial confirmation software, or similar verification method, to confirm participant's identity.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus uses facial confirmation software:

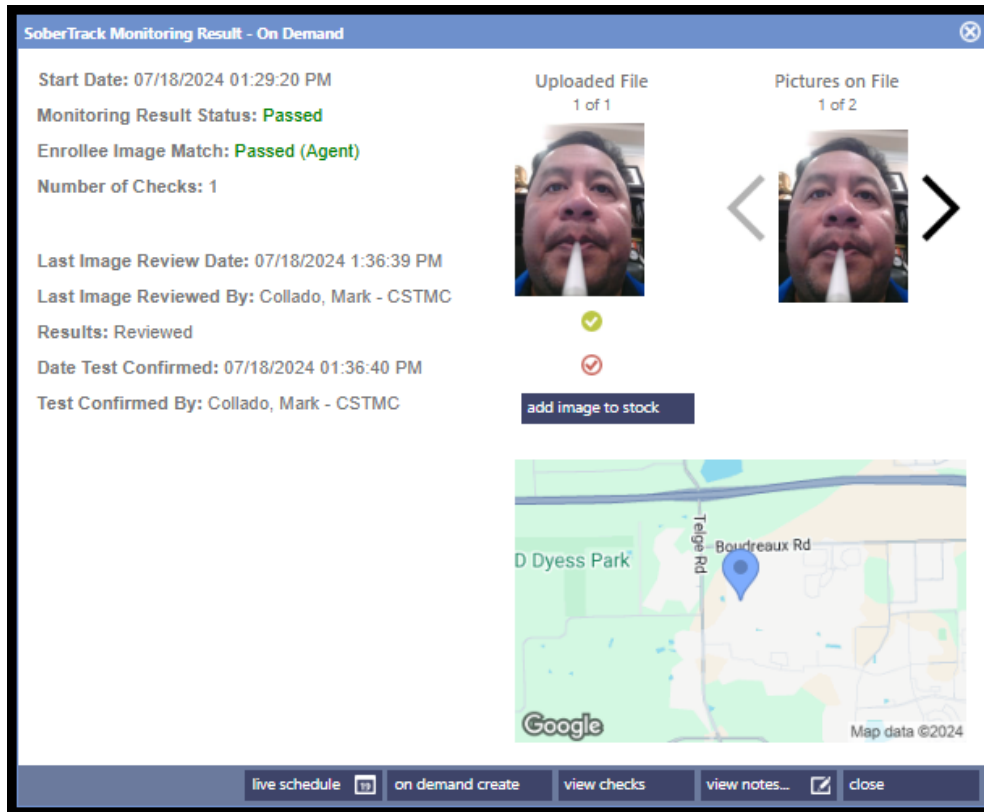
User Verification

SoberTrack utilizes a High Definition (HD) camera, which allows a detailed picture to be taken during testing. It also has LED backlighting that automatically activates for low light situations. These pictures are processed through automated facial recognition software and compared to previously uploaded photographs of the client as well as saved

photographs of the client taken over the last 20 tests. This comparison yields a pass or fail photograph.

An additional feature of SoberTrack is that failed photographs are automatically sent to our Solutions Center staff for a physical comparison and a final pass/fail evaluation prior to the photograph being made part of the client's record. This reduces false negatives for simple comparisons such as eyeglasses not worn, beard growth, and more. However, Securus can bypass the physical comparison and send all automated recognition failures to the field staff, depending on the needs of the customer.

Securus also employs an industry leading feature – video capture. Each test has a short stream of video taken before and during the test, and these video streams can be retrieved from the device by authorized users of VeriTracks. This capability will show much more information to supervising officers than a single photograph can provide.



SoberTrack client image is processed through facial recognition software. The device and software also allows an client's image to go through a match check by Securus Solutions Center Staff to determine pass/fail evaluation.

Device must collect the GPS location during the remote breath alcohol testing.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack excels at GPS tracking utilizing a unique feature that enables it to always be “online”. SoberTrack takes a single GPS location point each hour to validate its location and to stay current with the changing GPS environment. When performing a scheduled or random test, the device will update GPS coordinates in one-minute intervals for ten minutes prior to testing, during the test, and ten minutes after testing. The device is also taking single GPS locations during any missed test. This GPS location stream will enhance the ability of the supervising officer to evaluate overall activity and behavior while program clients are on the system. Additionally, field agents can request an updated location at any time to determine the device’s location between tests.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack® is a **GPS-enabled, cellular-connected** remote alcohol monitoring device that:

- Uses **cellular networks** to transmit test results and location data to **VeriTracks®**
- Collects **GPS location points** routinely and at higher frequency around test events
- Maintains near-continuous connectivity (“always online”) via cellular service
- Allows officers to request **on-demand location updates** between tests

SoberTrack does not require Wi-Fi connectivity, as all monitoring data is securely stored directly on the device and transmitted without reliance on local wireless networks.

Device must be lightweight, discreet, and easy to use, providing test notifications through push technology or SMS.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack is lightweight, discreet, and easy to use. It can easily be carried in the provided case or the client’s briefcase, backpack or purse. The optional SMS setup in our VeriTracks software can alert the client to a pending or missed test.

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).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack uses a U.S. Department of Transportation (DOT) approved alcohol-specific fuel sensor. It will reliably report Breath Alcohol Content (BrAC) as low as .01 with alerts customized by Participating Entity between .01 and .04 BrAC. The testing has been shown to have an accurate and direct correlation to blood alcohol levels.

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack transmits equipment data to include number of tests (which is used in calibration measurements), battery conditions, and tamper. All data reported is time-stamped and kept for officer review in VeriTracks. As SoberTrack is real time reporting, it uses cellular connection and does not rely on land lines for uploading.

Device must have a rechargeable battery.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

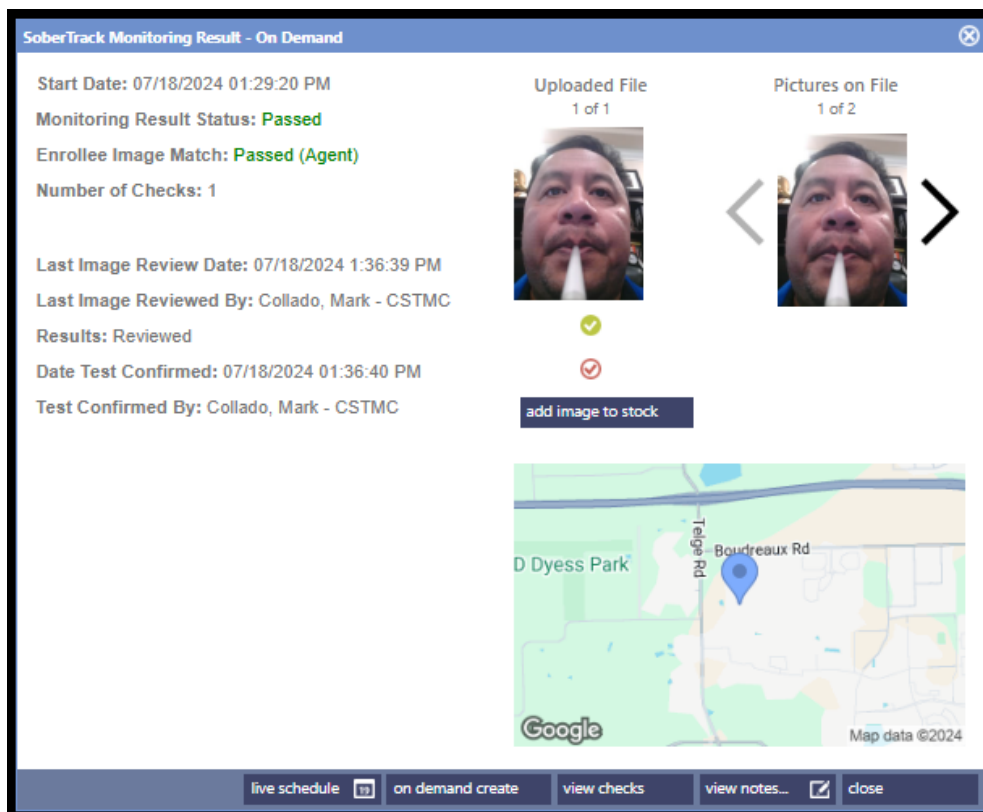
SoberTrack contains a lithium-ion battery that will maintain its charge for 48+ hours. To recharge the unit's battery, Securus recommends a charge time of two (2) hours. It has a sealed battery that lasts for 24 months and does not require field installation or service of the battery. Notifications alerting the supervising officer of the battery status are provided 30 days in advance to ensure the supervising officer has time to switch out the device. If a device has not been properly charged, it can go into a Low Battery Status. This generates an alert to the supervising officer; however, the device will continue to operate for up to ten (10) hours. This allows time to have the client charge the device, continuing participation in the program. SoberTrack will also provide tone and/or vibrations alerts to remind the client of the need to charge the device.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack immediately reports the results of any test and is available for review by the officer in VeriTracks. Tests include the result of the Deep Lung Sample of Breath Alcohol Content, a color image of the client who performed the test and the GPS location of the device where and when the test was taken.



Scheduled, Random & On-Demand Testing

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack can perform scheduled, random, and on-demand testing on a 24/7 basis, as the device is always connected to a cellular network. Each result is deemed passing, failed due to positive alcohol/other causes, or missed. All test results are immediately sent to the customer by email and/or text message for response after confirmation/review by our automated facial recognition software. Any failed images from automated recognition are

then sent to our 24/7/365 Solutions Center for a manual review of the image for a final determination of pass/fail before we alert the supervising officer.

In VeriTracks, schedules can be created to have clients perform up to 12 tests in a 24-hour period. On-demand testing can be created whenever the field officer or client deems necessary, on an ad hoc basis, up to 12 times in a 24-hour period as long as there are no other tests scheduled for the same time. Random testing can be set to administer up to three (3) tests during a given time frame, allowing for one (1) to four (4) hours between each test.

Tamper-Detect Features

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack is housed in a hypoallergenic, industrial-grade plastic case. Within that case, there is a light sensor. If the case is opened, SoberTrack detects the tamper attempt and immediately reports it to VeriTracks. A notification is then sent to the supervising officer and any other designated recipients through phone, text message, email, or fax, depending on the protocols set by Participating Entity.

SoberTrack also detects other attempts to defeat the device through such means as:

- Low air pressure
- High air pressure
- Short test time (i.e., under 4 seconds)
- Missed test (and retests)
- Failed image
- Low/Dead battery

Automated notifications and alerts (via SMS, email, or in-platform) for violations such as tampering, missed tests, positive test, or low battery.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

SoberTrack detects the tamper attempt and immediately reports it to VeriTracks, our web-based monitoring application. A notification is then sent to the supervising officer and any other designated recipients through phone, text message, email, or in-platform depending on the protocols set by Participating Entity. SoberTrack also detects other attempts to defeat the device through such means as:

- Low air pressure
- High air pressure
- Short test time (i.e., under 4 seconds)

- Missed test (and retests)
- Failed image
- Low/Dead battery

3. Customer Support and Training

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Monitoring Software (VeriTracks) will be available 24/7/365 for use. Below is a description of how we maintain our support throughout this time to provide service uptime for users.

Securus' dual-purpose Solutions and Monitoring Center, which is housed in our Houston, Texas, company headquarters, provides around-the-clock technical support to all customers. Securus employees staff the Solutions Centers 24 hours a day, 7 days a week and are on duty, rather than on call during overnight hours, weekends, and holidays. Our Solutions Center also has bilingual staff available, and other translation services are available upon request.

Securus follows industry-leading practices for hiring the most qualified personnel for all aspects of our company, including the maintenance, security, and integrity of our operations. All candidates must pass a comprehensive background investigation, including criminal records and drug screen, prior to an offer of employment. Before their first day of employment, they must also sign a confidentiality agreement. Upon request, we provide copies of background checks and confidentiality agreements. Additionally, access to the State's database is only provided to monitoring staff that are supporting the electronic monitoring program. If a third party, such as the court, attorneys, or law enforcement, requires information about an individual client, Securus requires a written request by State-authorized representatives.

Once hired, all Securus Center technicians are trained for a minimum of forty (40) classroom hours and forty (40) hours of side-by-side training with an established technician prior to receiving their certification. Each associate is trained on our operational procedures, which are also available on our online knowledge base within our ticketing system. Upon certification, technicians can provide Monitoring Center and support services to County staff.

Technicians can be reached by toll-free number, email, or fax for all requests. All calls are recorded and all telephone calls, text messages, emails, and faxes are stored within our Customer Relationship Management system, salesforce.com. These cases are date and time stamped with all information regarding resolution and action steps taken clearly presented and reviewable. We have also implemented a customer portal that provides State staff with the ability to directly access all ticket information and our on-line knowledge base.

Additionally, Securus-trained technicians are available in our parent company's Dallas-area headquarters to assume the Monitoring Center service and technical support functions of our Solutions Center in a matter of minutes. This additional backup resource is available today and ready to launch should the need arise. This resource can be activated for short-term, as well as longer-term operational issues with our Solutions Center. Should our Solutions Center need to relocate as part of our Disaster Recovery operations, our Dallas-based Technicians would provide the Monitoring Center service and technical support service to customers until our Houston-based Technicians arrive to the facility and are in place to resume their duties. If this is required, Securus will provide notification to the identified County Program Manager(s).



In 2020, our Monitoring Center technicians:

- Handled over 200,000 technical support cases, with 95% handled within two (2) minutes, 96% handled within five (5) minutes
- Processed over 30,000 device and supply orders
- Handled over 4,100,000 individual protocol steps for over 40 agencies

Our Solutions Center technicians respond to all types of requests about our monitoring system, including using the hardware and software; enrollment and un-enrollment; creating or editing zones and zone schedules; understanding monitoring data; interpreting maps, notifications and reports; determining the current location of clients; and troubleshooting issues. Many times, the questions are straight forward, such as moving a zone or changing the shape or schedule for a zone. Other times, a technician may lead a one-on-one mini training session on a specific functionality.

State-authorized personnel may contact the Solutions Center Technicians by email or by our toll-free phone number. All calls are answered immediately, and Securus' goal is to have all issues addressed within two (2) hours. For complex questions or issues, Securus' goal is resolution within 24 hours.

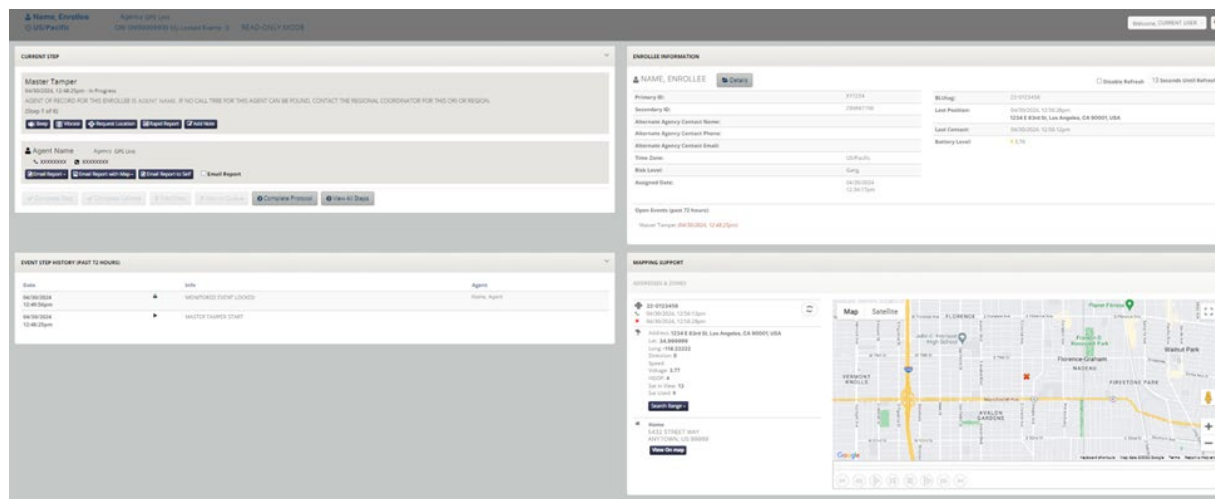
Our technical support is divided into three tiers.

- **Tier I Basic User Support Issues - Resolves more than 95% of the inquiries**
 - Solution Center technicians address questions about our hardware and software, provide assistance on all aspects of our system, including enrolling and un-enrolling clients; creating and modifying curfews, schedules and zones; interpreting data and maps; and determining the current or previous locations of clients.

- **Tier II Advanced User Support Issues - Resolve less than 5% of inquiries**
 - Solution Center software analysts address questions about our software. Also they receive the event notifications, such as tampering, identified by the Participating Entity and manage the event by following the customer-provided protocols. Handle data analysis, modification to VeriTracks layout, trending issue research, and provide direct customer support.

- **Tier III Non-Standard System Issues – Resolves less than 5% of inquiries**
 - Software Support Engineers respond to system availability issues, enhancement requests, firmware changes, Customer requested High-level VeriTracks customizations and implementations.

Securus works with the State to develop a unique set of protocols on how they would like their alerts to be processed. Alerts can be automatically generated immediately upon receipt from VeriTracks (our Host) through fax, email, or text message. Our 24/7 live operator Monitoring Center can also call the assigned supervision staff or the client. The events that generated the alerts are always visible in the dashboard through VeriTracks as seen below:



This screen capture displays the Monitoring Center component in VeriTracks that our Solutions Center Technicians use to provide Monitoring Center service. It lists the detailed protocol steps to take to manage the event, and a technician will check off each step as it is completed.

The Contractor must provide a dedicated account representative.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Each Participating Entity is assigned a specific Account Manager to serve as a trusted advisor. Account Managers are trained to work with the Participating Entity to help their program become successful. Examples include transitions, training, policies and procedures, etc.

The Contractor must provide support functions 24/7/365.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Supervising officers can contact our Solutions Center for technical support 24 hours a day, 365 days a year using our dedicated toll-free number or email address. All inquiries are entered into our ticketing system, which helps our technicians track the status of each inquiry. Our technicians can answer questions about our hardware or software. Instead of being limited to only verbal explanations for performing tasks, our technicians can also show supervising officers how to perform tasks by using GoToWebinar®, a secure online screen-sharing application.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Technicians can be reached by toll-free number or email for all requests. All calls are recorded and all telephone calls and emails are stored within our Customer Relationship Management system, salesforce.com. This information will be provided to Participating Entity upon award.

The Contractor must provide initial start-up training that must include but not be limited to the following:

The enrollment of clients into the software system.

The installation, use, de-installation, and cleaning of the equipment.

The generation and interpretation of data/monitoring reports.

Accessing/using Contractor's technical support/help menus and monitoring center.

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

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.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Initial training involves extensive hands-on handling and use of the equipment and software.

Training is a critically important foundational component to any supervision program. This is why we offer multiple types of formal training and numerous types of informal and self-paced training. We provide all training to the Participating Entity at no additional cost. This includes initial, refresher, follow-up and new officer training as well as train-the trainer training. We provide training guides, equipment and access to our secure web-based monitoring application. The Participating Entity provides the location(s) for the training, Internet access and a computer, laptop or tablet for every trainee.



Our designated transition account manager partners with the Participating Entity to ensure our training courses meet its needs and all identified personnel receive training. During the first phase of our Transition Plan, our transition account manager addresses the Participating Entity' training needs so they can be incorporated into the curriculum by our Training Department. Our trainers are knowledgeable and experienced Securus employees with years of experience in adult education and training. Because our trainers have been with us for years, they have extensive knowledge of our hardware and software and possess a deep understanding of customers' needs and expectations.

Initial training usually takes place on-site and requires a 1.5-day commitment for GPS monitoring equipment. Our comprehensive initial training course covers all aspects of our monitoring system, including:

- Enrollment
- Creating, assigning and editing zones and zone schedules and testing
- Understanding monitoring data
- Interpreting notifications and reports
- Determining the client's current location; and troubleshooting

Our training courses take a hands-on approach, so trainees use the actual hardware and software to explore the features and functionality of each component and build the trainees' confidence with our monitoring system.

While traditionally it takes approximately 12 hours to cover the required training, courses can be condensed to eight (8) hours for the training sessions. We can modify our training to meet the Participating Entity' needs.

We can provide on-site training for any class size; however, most classes have no more than 15-20 trainees. On-site class size is limited by the size of the training room and the number of computers, laptops or tablets the Participating Entity provides. We recommend classes with lower trainer-to-trainee ratios to allow for more one-on-one interaction between the trainer and trainees.

EXHIBIT 1: AVENTIV NIST ATTESTATION LETTER



August 15, 2025

To Whom It May Concern,

This letter informs you that A-LIGN Compliance and Security, Inc., an accredited FedRAMP Third Party Assessment Organization (3PAO), was contracted to perform a NIST 800-53 / FISMA Assessment on the IC++ System on May 15, 2025.

A-LIGN completed the assessment and provided Aventiv with a Security Assessment Report on August 15, 2025, the details of which are outlined below.

Dates of Testing: July 9, 2025, to July 25, 2025

Methodology: As described in NIST SP 800-53A, Revision 5

Scope: IC++

Objectives of Testing: To evaluate the security controls of IC++ for NIST 800-53/FISMA compliance.

The **IC++ system** delivers technology solutions for the public sector, supporting correctional operations and connecting incarcerated individuals with their families. It includes:

- **Securus Technologies** – Communication, security, entertainment, education, and re-entry services
- **JPay LLC** – Financial services for corrections
- **Securus Monitoring Solutions** – GPS-based electronic monitoring

Outcome / Disposition:

The IC++ system components were assessed according to NIST Special Publication 800-53 Revision 5. The security baseline controls define the policies, procedures, and controls an organization should have to comply with FISMA. The assessment results are as shown below:

Assessment Results	
Total Controls	287
Satisfied	249
Other than Satisfied	17
Not Applicable	21
% Satisfied	86.76%

Finding/Risk Level	Count	Percentage
High	0	0.00%
Moderate	3	16.67%
Low	15	83.33%



A-LIGN Compliance and Security, Inc.
400 N Ashley Drive, Suite 1325
Tampa, FL 33602

If you have questions or concerns, please contact me at melissa.curtiss@a-lign.com.

Thank you,

Melissa Curtiss
Federal Manager
A-LIGN, accredited FedRAMP 3PAO