

MARCH 16, 2023



AN RFP SOLUTION

NASPO Electronic Monitoring Products and Services
RFP – 22PSX0021

Response Requirement 1: Technical Document – Category
3, Global Positioning System Monitoring (“GPSM”)

PRESENTED TO:

State of Connecticut
Department of Administrative Services
Michael Baczewski
Contract Specialist
NASPO Value Point

PRESENTED BY:

Securus Monitoring
Greg Utterback
Chief Development Officer
5353 W Sam Houston Parkway North, Suite 190
Houston, TX 77041

REQUIREMENT 1: TECHNICAL PROPOSAL

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 1.0 Qualifications, Experience, General Requirements, and Industry Knowledge

Item	Requirement	Response
1.0	Describe proposer's qualifications and experience to provide the proposed Products and Services as an awarded Master Agreement Contractor for this Category of Need. Proposer shall describe qualifications and experience inclusive of specific public sector experience including project client, project scope, project budget, and timeframe over which the products and services were provided and/or performed. In particular, proposer shall highlight project experience working with states and/or other public entities including local governments over the past five years.	Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company, has been developing and marketing our GPS technologies for almost 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 and BLUhome® (home-based receiver) was introduced in 2006. 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. Examples of these programs, which range in average daily population from five (5) to 9,000+ offenders, include: 1. California Department of Corrections (CDCR) – 9,800 devices 2. State of New York Executive Department Division of Parole (NYDOCCS) – 595 devices 3. Orange County CA Probation Department – 250 devices 4. TN Office of Juvenile Justice – 250 devices 5. Hillsborough County FL Sheriff's Department – 80 devices 6. Arkansas Community Corrections – 510 devices 7. St. Lucie County FL Pretrial – 120 devices With a rich history of innovation that focuses on Agency needs, Securus Monitoring is a knowledgeable, resourceful, and responsive solution provider for these

		government agencies, as well as many others across the country. Since its inception, Securus Monitoring 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.
2.0	Proposer is expected to serve as a one- stop shop to meet all the requirements for this Category of Need and those requirements of this RFP. If proposer is unable to provide the full value chain of Products and Service the proposer may subcontract or partner with other entities to provide a specific Product or Service, or part of a Product or Service not 100% provided by the proposer. Describe how proposer will serve as a one-stop shop to provide proposed Products and Service for this Category of Need.	Securus Monitoring is the original equipment manufacturer (OEM) of all equipment described for this category of need: BLUtag, BLUhome, and BLUbox. We provide all consumables, such as straps (both DuraStrap and ToughStrap options) and clips, necessary to install and operate our equipment. Chargers, including mobile and car options, are provided as well. Our assembly and manufacturing operations are ISO 9001:2015-certified and based in Houston, Texas. We continually work with our vendors to ensure our inventory of straps, straws, motherboards, batteries, etc. remains in constant supply, and we have back-up vendors if necessary. As the original manufacturer, we have all the equipment ready and operational, so it is always available as the Participating Agency’s needs change. We also own, operate, maintain, and enhance VeriTracks®, our customizable monitoring application, which is updated at least three (3) times per year. We have dedicated IT resources that are experts in our software, which are also available to the Participating Agency to solve technical issues as needed. Additionally, we offer installation, case management, fee collection (if appropriate), disposition of violation

		notifications, and other services through our Solutions+ program, which is detailed in <i>Section 9: Optional Services</i>. We do not intend to use subcontractors to perform any work described in this category of need.
3.0	For this Category of Need, identify all subcontractor(s) by legal business name, including a contact name, email address, phone number and website. This list must include all subcontractors that proposer will utilize to implement, service and/or Perform the proposed Product and Service offerings.	Securus Monitoring does not use subcontractors on any of our current NASPO contracts and we do not intend to utilize subcontractors in the future.
4.0	Commercial Due Diligence: For this Category of Need, provide an analysis including but not limited to; social, political, and regulatory understanding of the electronic monitoring industry and the applicable laws, and regulations pertaining specifically to proposed Products and Services.	With almost 20 years of being in the Electronic Monitoring market, Securus Monitoring has been involved in many of the social, political, and regulatory needs that have impacted the industry. To this end, we contributed multiple times to the peer reviewed <i>Journal of Offender Monitoring</i> published by the Civic Research Institute. We have worked to align ourselves with our customers' mission and goals and ensure that our solutions contribute to their success. We meet all current regulatory requirements and have open dialogue with government agencies about appropriate uses and regulations. While we are politically agnostic, we are alert to any social and political changes; however, our focus is on our customers' success. Being an active member of the American Probation and Parole Association and the American Correctional Association and serving on several committees allows us to stay abreast and contribute to new developments, trends, and needs in the industry. According to the annual listing of laws and regulations on electronic monitoring compiled by the <i>Journal of Offender Monitoring</i>, there are few restrictions on the use of electronic monitoring to assist with the supervision of enrollees. While there is some disagreement amongst

		the major political parties about who should be supervised with electronic monitoring, there is concurrence that its use is appropriate when applied universally and not targeted to a specific group, such as low income or indigent. The National Institutes of Justice published a set of voluntary standards that set a baseline for devices. All Securus Monitoring devices comply with the applicable standards. Societal acceptance of electronic monitoring has mostly been increasing in the past few years. This increase in acceptance is partly the result of the ability to decrease the prison and jail populations by allowing increased community supervision.
5.0	Legal Due Diligence: For this Category of Need, provide an analysis including but not limited to; legal issues within the electronic monitoring industry and/or litigation pertaining to proposed Products and Services.	Securus Monitoring has never been found liable or guilty by a court of law. While we have been a party to litigation due to the nature of our business, these disputes usually involve issues that are resolved either outside the court through appropriate negotiations/mediation or Securus has been removed from the litigation by the court. Securus Monitoring is currently a party in limited litigation, but the outcome of these cases will have no material effect on our ability to perform under any contract or our ability to market and use our products and services. We offer all our customers expert witness testimony on our products and services. This testimony focuses on how our products operate and how the data is used for enrollee supervision. This is offered at no additional charge to our customers.

6.0	Products and Services: For this Category of Need, describe proposer’s expertise and qualifications in sourcing, delivering, implementing/ installing, servicing, maintaining, removing and disposing of proposed Products and Services, as applicable.	Securus Monitoring focuses on tailoring our hardware and software solutions to meet the evolving needs and expectations of our customers and supporting our monitoring program with extensive customer service. With almost 20 years of experience, and hundreds of customers, we are undeniably a leader in the industry. To support various customer requirements, we have made several modifications to our monitoring system and services to meet unique needs and expectations. We deploy these modifications throughout our system so that other Participating Entities can benefit from the upgrades. Examples of these enhancements are as follows: Manufacturing: We work with a variety of long-term vendors to ensure our inventory remains available to meet the needs of our customers. These vendors supply straps, clips, straws, motherboards, batteries, and wires. We also have a backup vendor for each item. We maintain a sufficient stock of all finished goods and consumables based on our current contracts and estimated future requirements. Additionally, we developed in-house capability of producing certain parts, such as chargers, to prevent stock shortages. When devices are returned from customers, all components are thoroughly inspected, cleaned, tested, and recertified for use in the field. While this initial NASPO contract requires all new devices, many customers accept the recertified devices for use in their programs since all devices shipped to customers are “like new” due to our recertification processes. Our standard shipping policy is to process and ship orders to customers within 48 hours of receipt Monday through Friday, 8 a.m. to 3 p.m. Central Time, except holidays. We use an international third-party shipping vendor for all our shipping and can ship next day air in urgent cases. Implementation/Transition/Service: In response to feedback during implementation/ transition, we have customized our system in several ways to meet a Participating Entity’s needs. We can reconfigure risk levels in VeriTracks to match established risk levels and
-----	---	--

		modify monitoring protocols to reduce the number of immediate notifications (if requested). As a result, VeriTracks immediately transmits only the most critical notifications to supervising officers. The rest are available when they log into VeriTracks. We also tailor existing reports and develop new ones to meet customer needs. We've successfully completed aggressive transitions in which we develop and implement customized monitoring protocols, train hundreds of personnel and assist with Product User enrollments and equipment installations. Utilizing our Application Programming Interfaces (APIs), we import a customer's extensive list of exclusion and inclusion zones to support monitoring of Product Users. Product Destruction: Securus Monitoring does not destroy our equipment as, in most cases, it can be recertified for use in the future (as described above). Devices that cannot be recertified, the components within the device are broken down and recycled with specific vendors for specific parts. For example, we have vendors that recycle our batteries and our plastic components.
--	--	--

7.0

Information Technology Solutions

For this Category of Need, describe proposer's expertise and qualifications in sourcing, delivering, implementing /installing, servicing, maintaining, and removing proposed information technology solutions including but not limited to any proposed Licensed Software.

Securus Monitoring has almost 20 years of experience providing electronic monitoring equipment and services. We obtained VeriTracks, our secure and reliable cloud-based monitoring application, in 2004, though it has been in use since 2000. More than 900 government agencies have used our comprehensive electronic monitoring system to monitor over 30,000 individuals.

SOFTWARE IMPLEMENTATION: In addition to adjusting risk levels, importing inclusion and exclusion zones, and customizing monitoring protocols, we have also enhanced our software with Global Zone creation, where we have built custom interfaces to import and setup/configure Global Zone data for Participating Entities. Each customer's requirements have varied slightly for related data (e.g., name, description, etc.) but the commonality between them is using the geospatial shape of the file format. This allows the user to create one inclusion/exclusion zone and apply it to one or more Product Users.

Case ID	Name	Agency	Case ID	Status	Event Type	Event Date	Event Time	Event Location	Event Status	Event Type	Event Date	Event Time	Event Location	Event Status
1000000001	JOHN DOE	Agency A	1000000001	Open	Location	10/10/2020	10:00:00	1000000001	Open	Location	10/10/2020	10:00:00	1000000001	Open
1000000002	JANE DOE	Agency A	1000000002	Closed	Location	10/10/2020	10:00:00	1000000002	Closed	Location	10/10/2020	10:00:00	1000000002	Closed
1000000003	JOHN DOE	Agency A	1000000003	Open	Location	10/10/2020	10:00:00	1000000003	Open	Location	10/10/2020	10:00:00	1000000003	Open
1000000004	JANE DOE	Agency A	1000000004	Closed	Location	10/10/2020	10:00:00	1000000004	Closed	Location	10/10/2020	10:00:00	1000000004	Closed
1000000005	JOHN DOE	Agency A	1000000005	Open	Location	10/10/2020	10:00:00	1000000005	Open	Location	10/10/2020	10:00:00	1000000005	Open
1000000006	JANE DOE	Agency A	1000000006	Closed	Location	10/10/2020	10:00:00	1000000006	Closed	Location	10/10/2020	10:00:00	1000000006	Closed
1000000007	JOHN DOE	Agency A	1000000007	Open	Location	10/10/2020	10:00:00	1000000007	Open	Location	10/10/2020	10:00:00	1000000007	Open
1000000008	JANE DOE	Agency A	1000000008	Closed	Location	10/10/2020	10:00:00	1000000008	Closed	Location	10/10/2020	10:00:00	1000000008	Closed
1000000009	JOHN DOE	Agency A	1000000009	Open	Location	10/10/2020	10:00:00	1000000009	Open	Location	10/10/2020	10:00:00	1000000009	Open
1000000010	JANE DOE	Agency A	1000000010	Closed	Location	10/10/2020	10:00:00	1000000010	Closed	Location	10/10/2020	10:00:00	1000000010	Closed

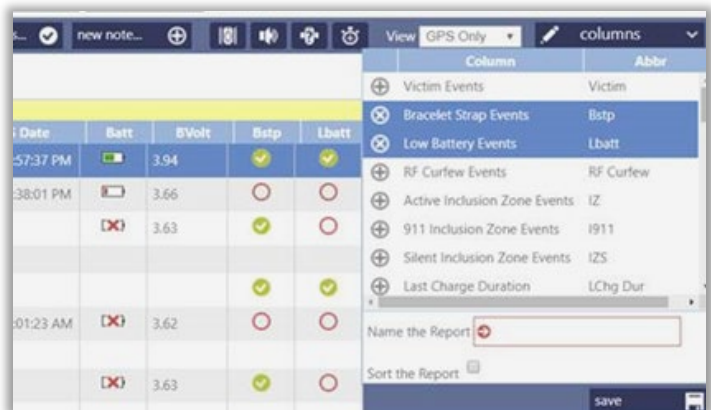


VeriTracks dashboard allows the Participating Entity's staff to quickly see who is active on their caseload, if there are any open events, and the last time the devices communicated with VeriTracks.

Further, the heart of VeriTracks is the customization that can be done within the application for each supervision staff user. The main screen within VeriTracks is the Dashboard. This is the screen staff see when they log into the application.

The ability to rapidly discern what events to take action with is easy to follow with the colored circles under the events. Participating Entity supervision staff can click on any of the circles to see additional information about the event and to also review the actions taken by our Monitoring Center. All contact with the Product User is accessible from the Dashboard, with dates and times of actions taken by our staff.

If the Participating Entity's staff is looking for Product Users that were previously monitored on VeriTracks, the filter options on the Dashboard make that easy to do. Choosing to see only the supervising staff's caseload, or everyone's caseload, is another view option within the Dashboard.



Customization of the view for each supervision staff is done from the Dashboard as well. The pictured drop-down menu shows which fields are available for the initial login view.

Since this is where most of a staff member's time is spent, VeriTracks also allows users to send the GPS device a tone or vibration alert, or to request the most recent position. All communication options are available from the screen.

Throughout its history, Securus Monitoring has partnered with customer agencies to provide customized integration with their case management or other data management

systems. We developed APIs (application programming interface) that offer a more standardized approach to data integration and provide them to a Participating Entity at no additional charge.

Examples of Existing Interfaces

CUSTOM

- Global Zones
- Data Export to an SFTP for Intoxication Monitoring
- Abscond Report
- SMS Client

STANDARD INTERFACES

- Automated Crime Scene Correlation API
- SFTP Bi-Directional Interface
- VeriTracks Data API

In some instances, the custom interface we developed for a particular customer agency ends up being a standard API, which we can provide to other customer agencies. An example of this situation involves our Automated Crime Scene Correlation (ACSC) functionality in VeriTracks. Because of an agency's integration effort, Securus Monitoring now has a standard "on-boarding" process for Participating Entities who want to integrate with the ACSC functionality in VeriTracks at no additional cost. The resulting API requires an integrating local law enforcement entity to produce only a comma separated value (CSV) file from their record management system and transfer it via secure FTP (SFTP) to our VeriTracks servers. Our standard integration platform then processes the file and runs the included crime incident data through our ACSC engine. Any matching Product User track point data or "hits" from the crime scene data are then presented to the parent agency that is partnering with the local law enforcement agency for further investigation.

We provide this information to show that not only do we provide customization of our solution, but also to show the value of these customizations.

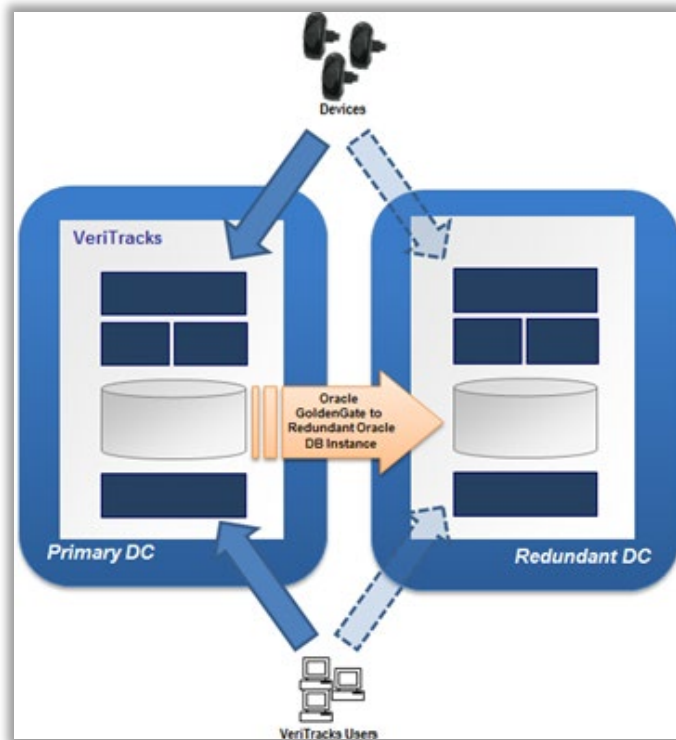
		MOBILE APPLICATION DEVELOPMENT: While details of our various applications are provided in Section 2.0-1, Securus Monitoring is aggressively improving and enhancing our mobile (smartphone) applications. We currently have two distinct mobile product offerings, one for agencies (VeriTracks Mobile) and one for enrollees (Enrollink). VeriTracks Mobile and Enrollink are both available on iOS and Android operating systems. IMPLEMENTATION/INSTALLATION/TRAINING: We revise our training curriculum and user manual as well as the delivery format for training Participating Entity personnel. For example, our dedicated account manager worked with CDCR's program management team for several weeks to develop and implement a customized training curriculum and delivery format. Even though this project required a significant investment of time and resources, the result exceeded CDCR's expectations. To this day, CDCR personnel continue to use these customized materials to train new supervising officers. We follow our proven implementation strategy using our Transition Plan (detailed in Appendix B). Through this transition plan, we coordinate and/or establish policies and procedures, implement monitoring protocols, train authorized Participating Entity personnel and assist with Product User enrollments and equipment installations at any of the Participating Entity's office locations. Data Retention/Destruction: Securus Monitoring does not destroy any data unless we receive detailed written instructions from the Participating Entity or another court of law. For the life of the contract, all monitoring data is assigned a transaction number and securely stored in VeriTracks and immediately accessible by authorized personnel. The accessibility of monitoring data applies to all Product Users in the customer's database whether they are currently enrolled and monitored with assigned equipment or have been un-enrolled. All Product User records are immediately accessible to all authorized personnel from any computer, laptop, smart phone, or tablet with a high-speed Internet connection.
--	--	---

8.0	Demonstrated Public Sector Experience and Performance. Proposer must have been in business for a minimum of five (5) years providing this proposed Category of Need and must demonstrate specific public sector experience as defined by having been legally contracted to perform work for a governmental client including but not limited to; a local and/or county, state or federal entity in the last five (5) years. Describe how proposer will meet this requirement.	Securus Monitoring has over 18 consecutive years of experience providing GPS equipment and services. Since 2004, Securus Monitoring, and our predecessor companies, has revolutionized the electronic monitoring industry with our patented pioneering one-piece GPS monitoring device, BLUtag. We have provided more than 900 Federal, state, county, and municipal agencies unparalleled service in support of their community supervision programs. This includes more than 50 current NASPO accounts encompassing more than 5,100 average daily units. In December 2013, Dallas, Texas-based Securus Technologies, Inc. (now Aventiv Technologies) acquired Satellite Tracking of People LLC 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 Satellite Tracking of People LLC remains a wholly owned subsidiary, cooperation with other Securus divisions has accelerated our product development and innovation in areas such as mobile applications and advanced data analytics.
-----	--	--

9.0	Product and Service Delivery and Performance Requirement: For this Category of Need, proposer 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. In addition, proposer's "brick and mortar" locations inclusive of all data centers must be based in the United States. Describe how proposer will meet this requirement.	MONITORING CENTER The Securus Monitoring electronic monitoring system, including our Houston, Texas-based Solutions Center, is available seven (7) days a week, 24 hours a day, with no gaps for holidays or weekends.  The Solutions Center 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 Participating Entity staff with the ability to directly access all ticket information and our on-line knowledge base. Each year, our technicians: • Handle over 200,000 technical support cases, with 95% handled within two (2) minutes, 96% handled within five (5) minutes • Process over 30,000 device and supply orders • Handle 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 offenders; 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. When Participating Agency-authorized personnel contacts the Solutions Center technicians, their 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 (3) tiers. Tier I Basic User Support Issues - Resolves more than 95% of the inquiries. Solution Center technicians address questions about our hardware and software, help on all aspects of our system, including enrolling and un-enrolling offenders; creating and modifying curfews, schedules, and zones; interpreting data and maps; and determining the current or previous locations of offenders. Tier II Advanced User Support Issues - Resolve less than 5% of inquiries. Solution Center software analysts address questions about our software. Also, they receive event notifications, such as tampering, identified by the customer 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. Security and Disaster Recovery – Monitoring Center If a disaster occurs and impacts our Solutions Center and power cannot be restored within a timely manner, our diesel-powered generator is activated. The generator is available to power the Solutions Center for 48 hours. If power is not restored within 24 hours, we can relocate its operations to a secondary location in less than 30
--	--	---

		minutes and be operational within minutes of relocating. In addition, our primary Solutions Center can also operate on a virtual basis by rerouting our toll-free telephone and fax numbers to a backup cellular telephone system without any disruption in service. As an additional precaution against interruption of service with our Solutions Center, our toll-free telephone and fax numbers can also reroute to our backup analog telephone system. Securus Monitoring-trained technicians are also 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, 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. DATA CENTER VeriTracks is designed using a Live-Live operational structure, which eliminates the need to back up the monitoring data generated by our customer's programs. Live-Live means VeriTracks is always operational in two geographically separated Data Centers and "live" at both locations. The Live-Live configuration ensures system administrators are always aware of the system's health and functionality. Other vendors rely on "hot-standby" architectures where they hope the standby system comes online in a time of crisis. With a Live-Live system, the redundant system is always available and in use. Securus Monitoring's data centers are in Carrollton, Texas and Atlanta, Georgia.
--	--	--



This configuration has many advantages. First, disaster recovery begins automatically and immediately. There is no switch to flip or any action to take. Because the backup system is always live, it is already running. Second, there is no chance the backup system will not start. Unlike a backup system that relies on a diesel generator, our Live-Live architecture is already operational and in use. Finally, restoration is easy and repeatable. The redundant chain is already scaled to handle the entire system's load. Service is not degraded as it is with the redundant systems of other vendors.

REDUNDANCY

All monitoring data is stored in VeriTracks, which is housed in our primary data center in Carrollton, Texas. In addition to the redundancy within a data center described below, our data center also has geographically redundancy in an alternate secure Atlanta, Georgia, site. We understand the need for a reliable system that includes plans for backups and disaster recovery. We have developed our systems, networks, and overall data center to provide the highest levels of reliability. In the event of any failure, our system has the highest levels of redundancy to provide

		for automatic fail over and recovery. Our system's reliability has three (3) important components: redundant networks, power and systems and data. Redundant networks VeriTracks is hosted in a facility that provides the utmost redundancy to create multiple routes for uninterrupted data transport around the globe. A diverse portfolio of carriers is used to create a network that is not reliant on any single Internet provider. If a carrier outage occurs, data simply reroutes to another path and continues flowing into VeriTracks. Redundant power VeriTracks is powered with redundant Power Distribution Units (PDUs). If the power is interrupted, all racks automatically switch to multiple (N+1) redundant Uninterruptible Power Supply (UPS) systems. Each UPS operates in hot-synch parallel. Additional spare capacity in both UPS power and non-UPS power is available. Each UPS module has its own DC battery bank with sufficient capacity to sustain the Data Center, HVAC, and other systems for up to 15 minutes (on full capacity load). In case of a power outage the UPS provides battery power until the Automatic Transfer Switch (ATS) switches over to multiple redundant 2-Megawatt Caterpillar Diesel Generators, which usually takes less than 15 seconds. All HVAC units, life safety and general-purpose loads in the data facility are also tied to the generator. Additional diesel fuel is stored on site to ensure at least 72 hours (about 3 days) of operation at full load. The Data Center has contractual arrangements with multiple vendors to ensure the generator is refueled and serviced as needed. Diesel generators are maintained and tested bi-weekly. Redundant systems and data Securus Monitoring architected completely redundant systems so if a hardware component fails, the system continues to operate normally while the failed component (a server or disk for instance) is repaired or replaced. Because the components we use in our architecture have their own internal redundancy (e.g., dual power supplies, processors, disks, etc.), in many
--	--	--

	cases we can resolve the failure by simply replacing its faulty hardware and this can be done without impacting its online and operational status. If for some reason the server itself fails in a manner that multiple of its internally redundant systems are compromised, we also have architected the layers of our application architecture to support a minimum N+1 redundancy model. This means that an entire server or hardware infrastructure component (e.g., switch, load balancer, etc.) can fail and become unavailable without impacting the services that VeriTracks offers. In addition to catastrophic occurrences with these components that can result in bringing them down this capability also allows the component to be brought offline for maintenance and upgrades without impacting the system's availability or degrading the overall performance of the application. The Securus Monitoring Data Center undergoes regular testing to ensure all systems function as expected should a natural or manufactured disaster occur. For example, in the past year alone Securus Monitoring has twice switched services and roles (i.e., primary vs. secondary) between its data centers ensuring that these procedures are documented and executed within acceptable time limits and with minimal disruption to the service. Using technology that broadcasts the target for their data, the Securus Monitoring fleet of devices can be diverted to the secondary data center. External access for VeriTracks and its related applications is then changed through the publishing of DNS changes that with a low time-to-live (TTL) can be quickly distributed to end users. Security and Disaster Recovery – Data Center Securus Monitoring provides the highest levels of industry-standard security measures to prevent hacking into the VeriTracks system and for the protection of the end-user and participant data. A subsidiary of General Dynamics designed and implemented our entire security model for VeriTracks. The same processes and procedures used to protect data for the U.S. Department of Defense and U.S. intelligence agencies were integrated into the development of the security protections for VeriTracks. We subsequently passed an
--	--

	audit to comply with the National Institute of Standards in Technology's (NIST) Special Publication (SP) 800-53 also known as FIPS 199. As part of our audit, we were classified with a Moderate Risk security classification per the standard. Only authorized users can log into VeriTracks. The program administrator creates a unique login ID for all authorized users. Access control lists (ACLs) and role-based access controls (RBAC) within the application control the level of access that users have to data and feature/function sets within VeriTracks. By default, the application also tracks login attempts and certain functions within the application such as mapping/viewing of offender data and can optionally be configured to track additional operations at the request of a customer should they have a reporting requirement for this data.  Our proactive approach to system security includes using industry-standard security measures to prevent unauthorized access to the data and implement fast recovery measures. VeriTracks provides a highly secure network environment monitored by skilled engineers and technicians. Our health monitoring system watches not only the operation of the servers and network but continuously checks our firewalls for attempted security breaches. In the event of a breach, automatic notifications are sent to our engineers. While Securus Monitoring has event escalation procedures in place for a security breach, we feel the best approach is prevention. We continuously monitor our security processes and procedures and update the overall security model as needed to address
--	--

		the newest threats. The Data Center security model is comprised of Network Security, Application 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 and create and modify data). Most users are created as normal users. Additionally, two-factor authentication can be utilized with VeriTracks, requiring the Participant Entity's 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 BLUtag and BLUhome 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 protected against physical intrusion by a well-known third party. They provide financial-grade protection for our mission-critical Internet operations. The centers are 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 Monitoring-authorized personnel have access to the cages in the Data Centers housing the VeriTracks servers. Both Data Centers have the following physical security measures:<table><tr><td>• Digital video monitoring and recording of entrances, exits and individual cages</td><td>• CCTV integration with access control and alarm system</td></tr><tr><td>• Card key (electronic badge) and biometric (fingerprint) access controls</td><td>• Mantraps at each entrance into and out of the facility</td></tr><tr><td>• Fire detection and suppression equipment throughout the facility</td><td>• Equipment checks upon arrival</td></tr><tr><td>• Shipping and receiving area walled off from co-location areas</td><td></td></tr></table> Our primary data center houses our Network Operations Center and shares a parking lot with our parent company's headquarters in Carrollton MANUFACTURING We also have plans in place should our primary manufacturing facility be rendered inoperable. Our plans	• 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	
• 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									

		include moving manufacturing to alternative sites available locally through our current landlord or to other lease facilities at least two hours away. These facilities are available to Securus Monitoring on short notice. We also have long-term arrangements to acquire and use generators during prolonged power loss. The Securus Monitoring recovery plan includes moving its inventory of available equipment to alternative sites and fulfilling customer equipment orders from those sites to continue business operations. OPERATIONS Securus Monitoring put its disaster recovery plan into action in 2017 when a hurricane hit the Houston, Texas, area. The hurricane left many parts of the city without power as well as serious flooding impacting many homes and businesses. Most of the roads throughout Houston remained impassable for more than one week. However, the Securus Monitoring production operations were minimally impacted and customers noticed little disruption. Our escalating disaster recovery procedures ensured partial or finished equipment moved out of the area before the hurricane hit. Once the storm passed through Houston, Securus Monitoring personnel moved the shipping operations to an unaffected site three (3) hours away and generators were installed in the Houston headquarters to resume operations at the headquarters. We have also put these plans into action in 2021 during a rare Winter storm in Houston, as well as utilizing remote operations during the COVID-19 pandemic, with no degradation to customers. A detailed copy of our Disaster Recovery Plan can be made available upon request.
--	--	--

10.0	Staffing and Project Management Requirements: Proposer must appoint Key Contractor Personnel, at no additional cost for the term of the Master Agreement. Key Contractor Personnel shall be the primary point-of-contact for all account- based customer service needs of the Participating Entity including but not limited to the scheduling of onsite visits, coordination of User training. Product User training, service request(s) and issue resolution. Proposer shall provide an adequate level of staffing required to fully and consistently provide all Products and Services and accommodate fluctuations in Participating Entity need. Proposer shall ensure that all proposer staff are fully trained, qualified, and licensed in order to comply with any Participating Entity specific requirements including background check policies. Proposer staff shall adhere to background checks at no additional expense to the Participating Entity. Describe how proposer will meet these requirements.	We have assembled what we believe is the most qualified electronic monitoring team in the industry today. Our executive team of corrections and technology professionals is unrivaled in its depth of experience and expertise. Each member of the team possesses extensive knowledge and experience in community corrections/ supervision including project management, program implementation, system integration, customer service, technical support, training, and contract compliance. We will utilize this collective experience to partner with Participating Entity's personnel to manage the monitoring of Product Users and maximize its resources, maintaining efficient operations during the life of the contract. By providing access to the entire account management team, especially during a transition to a new vendor, Securus Monitoring believes any Participating Entity will have a smooth transition. ACCOUNT MANAGEMENT TEAM The following key positions will support any Participating Entity's monitoring program: • Customer Success Manager (CSM) • Director of Field Support and Training • Solution Center Manager CUSTOMER SUCCESS MANAGER Our Customer Success Manager follows the Securus Monitoring project methodology approach and is accountable for understanding the customer's needs and any changes that are necessary. The CSM will facilitate any Securus Monitoring device and VeriTracks training as needed and ensures customers have the highest level of satisfaction with Securus Monitoring services, routinely reviewing account performance to ensure a successful program. The CSM works closely with each Participating Entity to learn about their infrastructure, policies, and procedures to ensure a smooth implementation and transition to Securus Monitoring. Additionally, the CSM has access to all Securus Monitoring resources – trainers, Solutions Center Technicians, fellow Account Managers (for assistance during large implementations), hardware engineers, and software developers – and can draw on them as needed.
------	---	---

		Many of our CSMs have more than 10 years of experience in supervising day-to-day operations of customer programs, data analysis, equipment installations and removals, inventory management, technical support, and training. They can also work with Participating Entity's to address legislative mandates and meetings with elected officials. DIRECTOR OF FIELD SUPPORT AND TRAINING Our Director of Field Support & Training has performed technical analysis, training, and field customer support, training adults employed in public agencies in groups as large as 100 or as small as five (5) and develops customized training curriculums for each Participating Entity by integrating their policies and procedures into the training materials. They possess extensive experience with adjusting high-end technology software and hardware into user-friendly and non-threatening subjects. This position oversees all trainers who provide the on-site initial and follow-up training, as well as intermittent online training sessions. Additionally, they ensure all Customer Success Managers respond to customers' day-to-day support needs. SOLUTION CENTER MANAGER Our Solutions Center Manager leads and manages our Solutions Center, which provides Monitoring Center service and technical support to customers 24 hours a day, 365 days per day. They ensure all Technicians receive comprehensive training on our hardware and software, as well as new equipment and functionality. They also work closely with the Training Department in developing ongoing training for the Solutions Center Technicians. The Solution Center Manager strives for new and innovative ways for the Solutions Center to grow and assist our clients in many ways while maintaining and keeping our promised SLA to each Participating Entity. ADDITIONAL ACCOUNT MANAGEMENT RESOURCES • Chief Development Officer • Vice President of Software Systems • Vice President of Hardware Engineering • In-house Legal Support
--	--	--

		Additional members of our NASPO account management team include our Chief Development Officer, who is the initial contact for the phases involving proposal evaluation and contract negotiations and signing. After the contract is signed, the lead contact is transferred to the Customer Success Manager. The Chief Development Officer will continue to serve as the Contract Administrator and maintain contact with the Participating Entity representative to ensure that we meet, exceed, and anticipate its changing needs. Securus Monitoring's Vice President of Software Systems will serve as the technical liaison for software functionality. The Securus Monitoring Vice President of Hardware Engineering is the engineer and technical expert in all aspects of our system hardware and its functionality. To ensure that Securus Monitoring meets any Participating Entity's potential need for legal support, we provide our in-house expert witness. They provide certification letters and expert testimony in defense of our GPS monitoring system when requested by Participating Entities or when subpoenaed. Finally, individual members of our Solutions Center staff may also be brought onto the team for various lengths of time throughout the account's life cycle. HIRING & TRAINING Securus Monitoring 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 and drug screen prior to an offer of employment. Upon request, we provide copies of background checks. Before their first day of employment, all Securus Monitoring employees must sign a confidentiality agreement. Upon request, we can also provide copies of confidentiality and non-disclosure agreements.
--	--	--

		All Solutions Center technicians are Securus Monitoring associates trained at least 40 classroom hours and 40 hours of side-by-side training with an established technician before receiving their certification. All associates are trained in our operational procedures and those procedures are available in our online Knowledge base within our ticketing system. Upon certification, technicians can provide monitoring and support services to a Participating Entity's staff. Our technicians are continually evaluated on their level of customer service, which is compared to the pre-defined metrics for the highest quality customer service. Throughout the year, technicians receive more than 80 hours of training through monthly and quarterly training sessions, which is in addition to the 80+ hours of initial training. Each agent meets individually with the Solutions Center Manager for an evaluation of the quality of customer service provided and training is adjusted as needed.
11.0	Compliance with Federal, State and Local Laws and Participating Entity Regulations: Proposer shall comply with federal, state and local laws and those regulations required by the Participating Entity. If awarded under this Category of Need, proposer must incorporate any new federal, state, or local regulations into their Products and Services at no additional expense to the Participating Entity. Describe how proposer will meet these requirements.	Securus Monitoring 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 Monitoring submits to annual audits and safety inspections, and we maintain our ISO 9001:2015 certification (recently renewed through December 2025). 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.

12.0	Describe proposer’s organization, including any parent companies, subsidiaries, affiliates, and other related entities. Include an organization chart showing each of the above referenced entities. Is proposer’s company publicly traded or is it privately held? Also, describe the ownership structure of Proposer’s organization, including any significant or controlling equity holders.	Since early 2005, Securus Monitoring, as Satellite Tracking of People LLC, has been providing government agencies and independent service providers with a proven and reliable electronic monitoring system, as well as providing a variety of services for supervising offenders in the community. In December 2013, Dallas, Texas-based Securus Technologies, Inc. acquired STOP as part of the strategy to expand its advanced technology product portfolio. While Satellite Tracking of People LLC continues to operate as a wholly owned independent division, Securus Technologies and its parent company Aventiv remains a privately held company through Platinum Equity. In 2022, STOP was renamed Securus Monitoring. The Executive Leadership Team reports to the Aventiv President and Chief Executive Officer. The Leadership Team consists of diverse and experienced innovators dedicated to delivering reliable and cost-effective communication and technology solutions within the corrections industry. Aventiv Organization Chart  <pre> graph TD DaveAbel["Dave Abel President and Chief Executive Officer"] CindyPechal["Cindy Pechal Chief Human Resources Officer"] AlexYeo["Alex Yeo Chief Product Officer and GM"] JoshMartin["Josh Martin Senior Vice President and General Counsel"] EvonJames["Evon James Chief Technology Officer"] MelanieSankaran["Melanie Sankaran Chief Information Officer"] MargitaThompson["Margita Thompson Chief Communications and Community Relations Officer"] JeramyCooperLeavitt["Jeramy Cooper-Leavitt Chief Information Security Officer"] AlexanderDougherty["Alexander Dougherty Chief Operations and Strategy Officer"] DaveAbel --- CindyPechal DaveAbel --- AlexYeo DaveAbel --- JoshMartin DaveAbel --- EvonJames DaveAbel --- MelanieSankaran DaveAbel --- MargitaThompson DaveAbel --- JeramyCooperLeavitt DaveAbel --- AlexanderDougherty </pre>
------	--	---

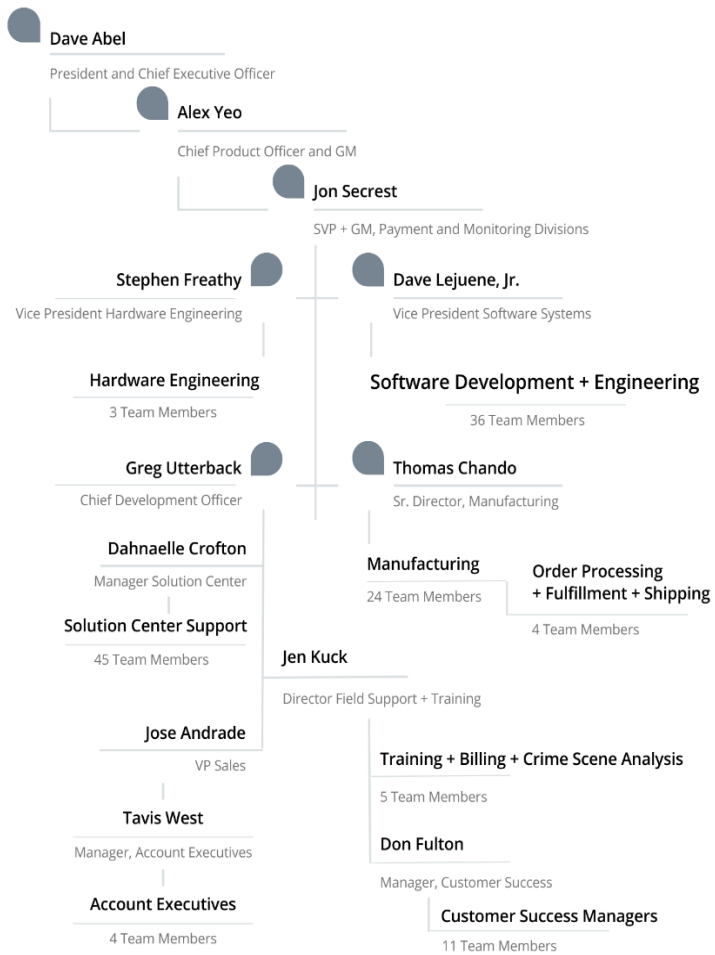
		EXECUTIVE MEMBERS David Abel, President and Chief Executive Officer, has 30+ years of public and private sector technology experience including criminal justice, law enforcement, national security, and intelligence. Dave started a successful automation and artificial intelligence business, was a partner at PricewaterhouseCoopers, and was an executive in the U.S. and overseas with IBM where he was the General Manager, U.S. Public Sector, with revenue over \$2 billion and a team of more than 4,000. Alex Yeo, Chief Product Officer and GM, has 20+ years of public and private sector technology experience including retail, consulting, and operations. He has a successful operations and product manager background, including being an executive in the U.S. and overseas with McDonald's where he was the Managing Director and VP, with revenue over \$1 billion. Alex Dougherty, Chief Operations and Strategy Officer, is an experienced strategist and change leader. He began his career in financial analysis in the defense industry and then guided transformation in diverse industries while in leadership roles at a leading consulting company. Prior to joining the Aventiv Team, Alex was Vice President, Transformation, at Platinum Equity, the private equity owner of Securus Technologies. Evon Jones, Chief Technology Officer, has 30+ years of information technology and CIO leadership experience in diverse industries including investment banking (Lehman Brothers), financial services (American Express), transportation (America West Airlines), and consumer brands (Hallmark, The Dial Corporation, Bausch + Lomb, and Liz Claiborne). Josh Martin, Senior Vice President and General Counsel, is an attorney with 20+ years of experience advising companies on dispute resolution and strategic initiatives. Prior to joining Aventiv in 2016, Josh practiced as a commercial litigator with global law firms, and he excels at finding creative, practical, and business-oriented solutions to complex legal problems.
--	--	--

		Cindy Pechal, Chief Human Resources Officer, has 30+ years of leadership experiences in human across diverse industries, including technology, banking, professional services, and life sciences. She has guided companies through mergers, acquisitions, divestitures, employee engagement initiatives, diversity awareness, and corporate transformation throughout her career. Prior to joining Aventiv, Cindy was the owner of a consulting company specializing in organizational effectiveness and talent management. Melanie Sankaran, Chief Information Officer, is an industry recognized cybersecurity leader with 20+ years of experience across multiple industries and technology layers. Previous roles include Vice President of Cyber Operations at Fidelity Investments and leadership at Experian where she directed Information Security for North America and Application Security globally. Melanie also held various information security roles at Wells Fargo Dealer Services, Foundstone, and Ernst &Young. Jeremy Cooper-Leavitt, Chief Information Security Officer, has 20+ years of international success in implementing strategic-level IT plans including network migration, security consulting, SOX compliance implementations, IT Governance, Payment Card Industry Compliance, and Privacy Law compliance (International and US privacy laws). He has been instrumental in developing the Cyber program, bringing stability and acceleration to key initiatives and overall leadership of the team since joining Aventiv. Margita Thompson, Chief Communications and Community Engagement Officer, has 25+ years of communications, public policy, and community engagement experience across federal, state, and local governments. In the private sector, she has worked in industries crossing energy, entertainment, real estate, and technology. Among previous positions, she served as Press Secretary for California Governor Arnold Schwarzenegger, political producer at CNN for Larry King Live, and as a public affairs leader at Fortune 500 companies, including Disney and Health Net. Most recently, Margita was Senior Vice President of US Corporate Communications at Unibail-Rodamco-Westfield.
--	--	--

	The following members of the Senior Leadership Team contribute significantly to our customer service and product development. Jonathan Secrest, Senior Vice President and General Manager—Public Sector Solutions, joined Aventiv over seven years ago and reports to the Chief Growth and Product Officer. He has 25+ years of experience in senior leadership positions in marketing and operations, successfully driving growth in technology manufacturing and telecommunications, including roles at TE Connectivity and Eschelon Telecom. Jessica Lust, Senior Vice President and General Manager—Technology, Media, and Entertainment, has 15+ years of experience leading projects and teams in the brand merchandizing and telecommunications industries. In addition, she previously served as the Director of Client Services for JPay, Inc., a Securus Technologies subsidiary and the industry leader in corrections communications and payment technology. ADDITIONAL SECURUS MONITORING RESOURCES • Greg Utterback, Chief Development Officer • Dave Lejeune, Jr., Vice President of Software Systems • Stephen Freathy, Vice President of Hardware Engineering Greg Utterback, Chief Development Officer, is the initial contact for the phases involving proposal evaluation and contract negotiations and signing. After the contract is signed, he hands off the lead contact to the Customer Success Manager (CSM) to manage the Participating Entity's program. Mr. Utterback, with support from the CSM, will continue to serve as the Contract Administrator and maintain contact with NASPO representatives to ensure that we meet, exceed, and anticipate any changing needs. Dave Lejeune, Jr., Vice President of Software Systems, will serve as the technical liaison for software functionality.
--	---

Stephen Freathy, Vice President of Hardware Engineering, is the engineer and technical expert in all aspects of our system hardware and its functionality.

More information about backgrounds can be provided upon request.



13.0	Scenario: An incumbent contractor on the current Washington NAPSO ValuePoint Master Agreement for electronic monitoring in a given Participating Entity is no longer on the 22PSX0021 Master Agreement and the Participating Entity executes a Participating Addendum with your company as an awarded Contractor. Describe how as an awarded Contractor proposer will work with the incumbent contractor and the Participating Entity to ensure a transition that is in the best interest of the Participating Entity. Attach a transition plan which documents that proposer would implement to ensure key milestones, user acceptance testing and staffing strategies and successfully provided to the Participating Entity undergoing this hypothetical transition.	Securus Monitoring has successfully transitioned many programs, both small and large, from other vendors that required extensive coordination between our organization and the customer. Due to the various nature and scale of these projects, not only do we apply the best practices in project management, but through a proven process, we guarantee the execution and timely deployment of all units for the Participating Entity. Securus Monitoring proposes a four (4)-phase project management approach when we are awarded a contract for Electronic Monitoring Equipment and Services, whether it is a new program or transitioning from a previous contractor: Program Management, Pre-Enrollment, Enrollment, and Ongoing Operations. We provide this information to all customers so they may understand our solid approach to implementation and to set expectations going forward. While our implementation schedule can range from two weeks to 60 days, depending on the number of people to be trained and devices to be transferred, we recognize the customers have diverse needs and our project timeline reflects that. To ensure a smooth implementation from an incumbent contractor, Securus will work with both the Participating Entity and the incumbent to understand current protocols, data transfers, application integration, and specialized data monitoring fields and reports. Using this information, our technicians will create the Participating Entity's database and test all aspects to allow users to feel comfortable with transition. Once the Participating Entity approves the electronic monitoring database, our trainers will provide in-depth training on both the hardware and software as described in Section 7.0: Product and Service User Training. Our customizable transition plan has been provided in Appendix B.
------	---	--

14.0	Transition Planning: The current NASPO ValuePoint Electronic Monitoring contract is set to expire 05/30/2023 and Master Agreement awards for 22PSX0021 are intended to be made in early May 2023. Describe how proposer will allocate the appropriate resources including account management, legal and administrative staff to effectively and efficiently execute Participating Addendums with Participating Entities. What do Participating Entities need to know to efficiently and effectively identify, implement and maximize utilization of proposed Products and Services under this Category of Need?	Once the new NASPO agreement is awarded, Securus Monitoring will transition our existing NASPO customers over to the new agreement. To make this an efficient process, with little to no impact to the current Participating Entities, we will: • Facilitate communication through our account management team (Customer Success Managers) by engaging the Participating Entity on the NASPO agreement to obtain new signed participating addendums. As our CSM teams regularly communicate with their customer base on several topics including contractual agreements, this process is expected to proceed expeditiously. • Advise Participating Entities that are already using RF and GPS products through the current NASPO agreement of any new products added to the new NASPO contract (22PSX0021) for them to utilize now or in the future, in addition to being advised of any new terms and/or new pricing that may affect their current contract. When the recent extension was provided to support the development of the new Master Agreement/Contract 22PSX0021, this process was completed in less than two weeks for all current customers. Our CSMs, Contract Manager, and other administrative staff are already in place to ensure a successful execution of the Participating Addendums for the new contract and will have all Participating Entities moved to the new contract within four weeks.
------	--	--

15.0	For this Category of Need, what factors contribute to the reliability and Uptime of proposer's Products and Services? Are there specific geographic areas of the United States where proposed Products and Services do not work or do not perform with 100% availability?	Independent tests, based on a 24-hour test period when the Securus Monitoring GPS devices has an unobstructed view of the sky with ideal atmospheric conditions, confirm: • Our device acquires a GPS signal within two (2) minutes • Device obtains one GPS location point per minute 99 percent of the time • The GPS location points are 95 percent accurate within a range of 10 meters (33 feet) Since our products rely on satellites and cellular networks that are out of the direct control of Securus Monitoring, there may be areas of the United States that do not have 100% availability. Although our devices offer robust cellular capabilities, some areas are outside of coverage. This will require the use of a landline option (if available) or the devices will store the data and transmit when cellular coverage is available. Coverage maps are available for both AT&T and Verizon for agencies and our CSM staff to assist with the utilization of our products where cellular coverage is limited.  Horizontal Dilution of Precision (HDOP) Rating Scale The accuracy of GPS location points is dependent on the geometry or proximity of multiple GPS satellites to each other and how many satellites a receiver sees at any given time. When visible GPS satellites are close together in the sky, the geometry is said to be weak and the DOP value is high; when far apart, the geometry is strong and DOP value is low. HDOP can be used to determine the accuracy of the GPS point and highlight areas of limited GPS availability.
------	---	--

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 2.0 Data Use, Supply Chains, and Information Technology

1.0	Scenario: I am a Product User who must wear and/or use the proposed Products and Services. Proposer Response to: For this Category of Need, and for each proposed Product and/or Service proposed under this Category of Need, explain how my data is: 1. Extracted by the proposed Products and Services. 2. Stored by the proposer, proposer's subsidiaries, affiliates and/or other entities and those of any subcontractor(s). 3. Utilized by the proposer, proposer's subsidiaries, affiliates and/or other entities and those of any subcontractor(s).	VeriTracks, Securus Monitoring's secure web-based monitoring application, is the repository of all Product User data (e.g., name, phone number(s), address(s), risk level, physical characteristics, photo(s), etc.) and monitoring data (e.g., GPS location points, curfew violations, tamper alerts, zones, zone schedules, etc.). VeriTracks will distribute event notifications, such as tampering and curfew violations, to unlimited designated recipients, including victims and alternate contacts, by any combination of email, fax, phone, and/or text message. Each Participating Entity recipient can choose how to receive event notifications, but the selections must comply with any protocols established by the Participating Entity. It is available 24 hours a day, 365 days a year to authorized personnel from any computer, laptop, smart phone, or tablet with a high-speed Internet connection. Following are the common functionalities used in VeriTracks: • Enrolling and un-enrolling individuals into and out of Participating Entity's electronic monitoring program • Creating and assigning date and time sensitive zones, which are geographic areas Product Users are either required to enter and remain for a pre-determined amount of time or prohibited from entering for designated hours of the day • Creating and adjusting an unlimited number of curfew/absence periods for each Produce User • Display, analyze, and evaluate monitoring data and Product User locations and movements on Google Maps™, including StreetView where available • Generate various reports that reflect near real time
-----	--	--

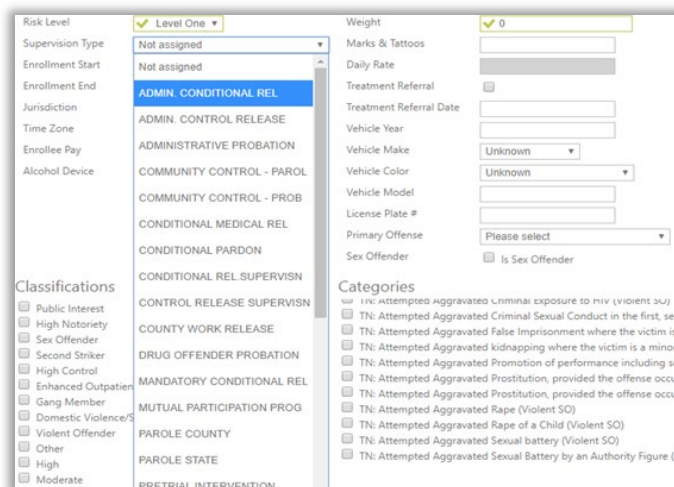
4. Protected by the proposer, proposer's subsidiaries, affiliates and/or other entities and those of any subcontractor(s).



Product User Information

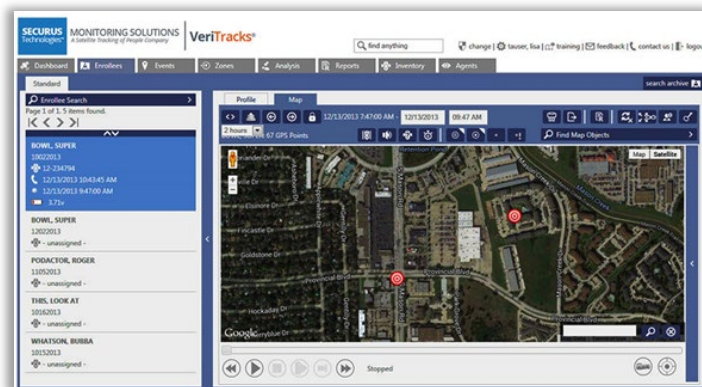
VeriTracks is highly customizable to a Participating Entity's needs both in the beginning of the contract, when the database is set up, and throughout the contract, as user needs change. Data fields and information stored, at a minimum, include the following:

- Agency name, address, telephone, fax, and pager numbers
- Group agency name and address
- Monitoring configuration parameters
- Field equipment parameters
- Alert Processing standards and procedures
- Officer name, address, telephone, fax, and pager numbers
- Product User's name, address, phone number, supervising officer
- Monitoring Equipment IDs, configuration, and inventory reports
- Unlimited number of enrollee schedules/curfews
- Staff notes
- Risk/need level of each Product User



In addition to the above, any Participating Entity personnel can login to VeriTracks and update or add multiple photos of subjects. VeriTracks immediately records these changes and are accessible and part of the enrollee's electronic record.

VeriTracks displays the location and movements of Product Users on Google Maps™, which has the same functionality and map perspectives as the ones on the commercial Internet version, including StreetView. Participating Entity personnel can view the location and movements of one or more enrollees simultaneously on a map and print the map directly from the screen. The movements can be selected based on date and time and can be viewed in a small timeframe, such as a five-minute span, or as long as 24 hours. Authorized personnel can also establish customized monitoring parameters for each enrollee. For example, GPS zones and zone schedules are date-and-time-sensitive to meet the unique needs of each enrollee.

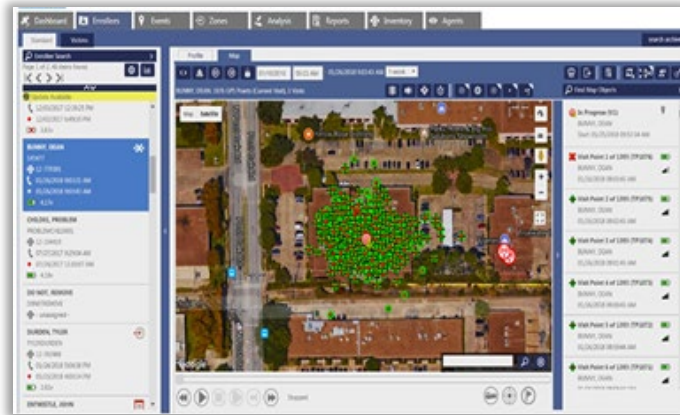


REPORTING

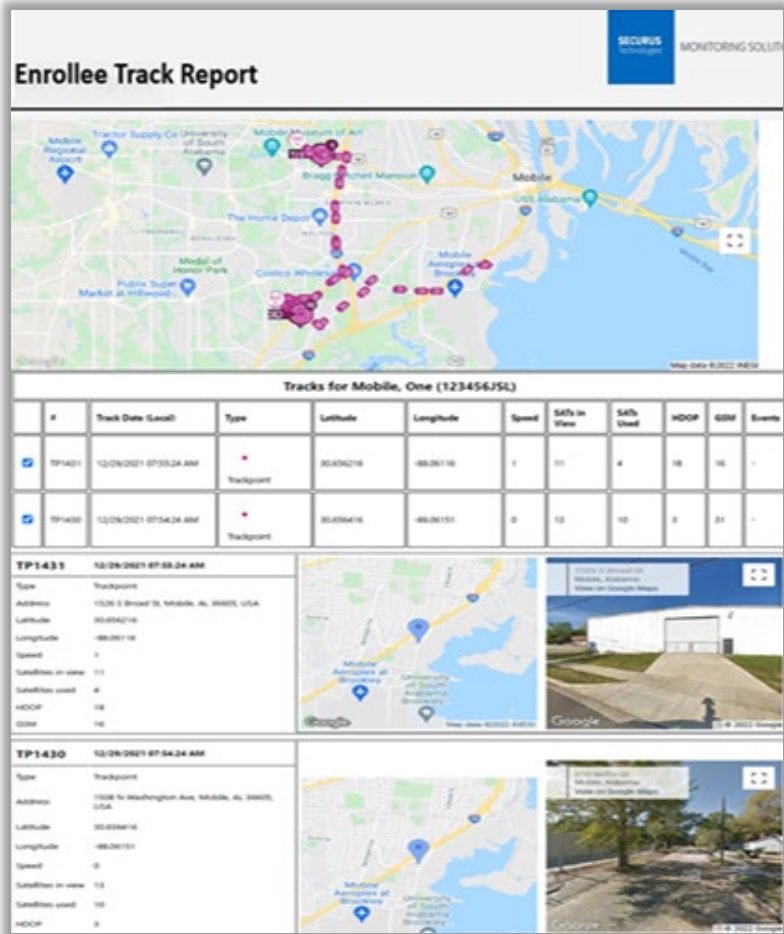
In addition, VeriTracks can produce more than 300 automatic standard reports, as well as ad hoc reports. When Participating Entity personnel login to the web-based application, they can generate reports reflecting real time data. Reports can be sorted or filtered using any field. They can also be filtered to reflect data for a single user, a group of users, a geographic region, or the customer's entire program. VeriTracks automatically stores a copy of each generated report for future reference. Authorized personnel can print reports from the screen or export them in several common formats, including Microsoft Word and Excel, PDF, and comma delimited.

Customers can restrict access to certain reports. For example, VeriTracks contains a wide variety of reports related to program

management. The customer may want to restrict access to these reports to program administrators who can generate them.



Offender location information can be displayed in a sequenced manner or provided for specific date and times, depending on the needs of the supervising agent.



		Offender information including events and GPS locations can be displayed in a report with a map based on specific date and times, depending on the needs of the supervising officer. MOBILE APPLICATIONS PRODUCT USER APPLICATION – ENROLLINK Securus Monitoring offers a mobile application specifically developed for the Product User called ENROLLINK. With Enrollink, available in the Google Play or iOS App Store, the Product User can request schedule changes and update their photos within VeriTracks, upon supervision staff approval. Enrollink can be used to receive additional information from the Product User including random GPS checks through additional location requests and the requirement to contact the assigned supervision staff. The supervision staff can also send a note to the Product User through VeriTracks to Enrollink. OFFICER APPLICATION – VeriTracks Mobile Securus Monitoring 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 Product Users 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 the data. VeriTracks Mobile offers the exclusive 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. DATA SECURITY Securus Monitoring's Data Centers, located in Carrollton, Texas and Atlanta, Georgia, are secured against physical intrusion by a well-known third party that secures some of the nation's most sensitive information. They provide financial- and military-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 multiple physical security features including anonymous windowless exteriors, Kevlar-lined exterior walls that are bullet resistant, security access control and alarm system integrated with closed circuit television, interlocking "mantrap" doors, and biometric hand-geometry scanners. Our primary Data Center is classified as a national asset by the federal government. In the event of a crisis, the National Guard rallies at the facility to protect it. It has an extensive history in information security and currently supports some of the most classified facilities and programs in the country. Only our system administrators have
--	--	---

		access to the center and their access is strictly monitored and recorded for future reference. The exchange of monitoring information between authorized Participating Entity personnel and Securus Monitoring 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. DATA PRIVACY All data remains the property of the Participating Entity. This data is not shared with Securus Monitoring's parent company, nor is it shared with any other party or agency except with the specific written request from the Participating Entity or a properly executed subpoena.
2.0	Is artificial intelligence employed by proposer for any Products and Services under this Category of Need? If yes, please explain.	Securus Monitoring 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 they are compliance with their conditions of supervision and successful with reintegration.
3.0	For Products and Services proposed under this Category of Need, what country(ies) are Products and/or Services or components of Products and Services sourced from? Describe the reliability of proposer's Product and Service supply chain(s).	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 Monitoring 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 our straps in bulk, with most orders being over 20,000 individual straps.

4.0	What are the greatest risk(s) to proposer's Product and Service supply chain(s)? How will proposer meet an increase in demand for Products and Services under this Category of Need?	Securus Monitoring has established stocking levels for all finished goods and consumable items, which allows us to meet increased demands as they arise. If a large quantity is required and not currently in stock, our manufacturing team can quickly move to three (3) shifts to meet demand. Our inventory of components and consumables is easily increased due to our long-standing relationships with our suppliers. Securus Monitoring maintains an average of three-four (3-4) month's supply for all consumable products in our warehouse in Houston. In the event of an increased demand, we can draw down this inventory while increasing our production capacity. The greatest risk to our Product and Service supply chain is shipping. With the large quantities of goods that we procure at one time, these goods are often shipped by boat or air. The boat schedule is less regimented than air or ground freight, so there are times that our deliveries are later than we expect. Our advanced planning allows for these large variances in delivery times. We also have the option to ship our products by other means, as necessary.
5.0	Describe the primary cost drivers for the proposed Products and Services under this Category of Need.	Primary cost drivers for all Securus Monitoring devices and services are labor for engineering design and manufacturing, material costs, testing, quality control, and certification.
6.0	Describe the proposed methodology to protect the security and confidentiality of Product User and User data and information proprietary to Participating Entities or subject to special statutory protection, including but not limited to; Product User personal information, personal identifiable information and health information. 1. Describe proposer's experience, qualifications and capabilities in protecting highly sensitive and confidential information.	Securus Monitoring takes a proactive approach to application and network security and upgrades our security measures on an ongoing basis. We use industry-leading technology and tools to provide the highest levels of security to protect the monitoring data and Product User personal information, prevent hacking into our monitoring system, and implement fast fault recovery. Our system's security model was designed by a 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. More information about our application, network, and physical security, including our Disaster Recovery Plan, has been provided in Section 1.0-9.

	Is the proposer a business associate as it relates to HIPAA?	To support secure transmissions, the exchange of monitoring information between authorized Participating Agency 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. VeriTracks' standard configuration for all access is two-factor authentication provided by Google, but this can be disabled at the request of the Participating Agency. Securus Monitoring also 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 and drug screen prior to an offer of employment. Before their first day of employment, they must also sign a confidentiality agreement. Our employees understand the importance of maintaining offender confidentiality and are trained in HIPAA (although minimal, if any health information is collected) and PII requirements. Upon request, we provide copies of background checks and confidentiality agreements.
--	--	---

7.0	For proposer staff that work remotely and/or telework, describe how proposer safeguards Product User data and User data and other data deemed necessary to be protected by the Participating Entity.	All staff use laptops with special software that does full disk encryption. In addition, connecting via VPN to the corporate network requires MFA (multi-factor authentication). All account holders must use strong passwords for logins, which are changed every 90 days. All laptops have remote patch management to stay current with the latest security updates and have EDR (endpoint detection & response): next generation anti-virus and anti-malware software, to proactively detect and remove malicious software. If a laptop is lost, stolen, or somehow compromised, it can be locked out of the network, and a remote wipe command can be issued. Our company maintains strong access control policies to prevent unauthorized access to data and systems. All associates must successfully complete a thorough background check prior to employment. Access to business information systems is provisioned based on the job functions of a role, using the principles of least privilege and separation of duties. Associates are required to complete the corporate Information Security online training course on an annual basis. Furthermore, all
-----	--	--

		associates must annually certify in Cybersecurity Awareness training, which trains every associate in Cybersecurity best practices. This Security Awareness training covers common security threats, disaster recovery and incident response, insider threat, proper data handling, and corporate policy review. This also includes mandatory phishing campaigns conducted at least bi-annually. In addition to attending annual training sessions, the Corporate Information Security team keeps up to date with emerging security trends.
8.0	Describe current security screening practices for proposer's employees, and any ongoing security screening that may take place during the Master Agreement term. Include a description of any security clearances or certifications that proposer requires of its employees.	Securus Monitoring 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 and drug screen prior to an offer of employment. Before their first day of employment, they must also sign a confidentiality agreement. While our employees do not require any certifications, our Solutions Center staff goes through rigorous initial training, as well as ongoing annual training, to ensure we meet customer knowledge expectations. Upon request, we provide copies of background checks and confidentiality agreements. The Participating Entity has the discretion to require us to disqualify, prevent, or remove any employee from performing any work under this contract.
9.0	Is proposer SOC 2 compliant? If yes, please explain how and provide proof.	While Aventiv (our parent company) is SOC 2 and SOC 3 compliant, VeriTracks is not currently being evaluated for SOC 2 compliance. If the State (or other awarding agencies) is willing to sign a non-disclosure agreement (NDA), or can demonstrate that one is in place, we can provide them with the latest Aventiv SOC2 Final Report.
10.0	Has proposer or a subcontractor which proposer will utilize under this Master Agreement been subject to a data Breach in the last 12 months? If yes, please describe the breach incident(s).	Securus Monitoring has never had a breach of data.

11.0	Does proposer have cyber insurance? If so, please provide proof including a copy of proposer's certificate of insurance and the declaration page. This information will be kept confidential.	
12.0	How will proposer ensure a Participating Entity can audit the reliability and uptime of proposed Products and Services under this Category of Need?	Upon execution of an NDA, Securus Monitoring will allow Participating Entities the opportunity to review the logs that record and evaluate our reliability and uptime. These logs will be available over Microsoft Teams or in person at our Carrollton office. Our internal and external audits are also available for limited review.
13.0	What reporting will proposer provide to a Participating Entity to document compliance with Exhibit C. requirements for Uptime and System Availability?	Upon successful negotiation of the Master Agreement, Securus Monitoring will create and provide the following reports: • Daily Report - A daily report describing the System Availability and performance of VeriTracks during the previous 24-hour calendar day as compared to the System Availability requirement will be sent by 10:00 a.m. on normal business days. • Weekly Report – A weekly report describing the System Availability and performance of VeriTracks during the previous seven (7) calendar days as compared to the System Availability requirement will be sent every Tuesday by 10:00 a.m. Eastern Standard Time (EST) and will include the previous seven (7) calendar days (Monday through Sunday). The reportable week shall begin at twelve (12 a.m.) EST, and end midnight (12 p.m.) Sunday of that calendar week. • Monthly Report - A monthly report describing the System Availability and performance of VeriTracks during the calendar month as compared to the System Availability requirement will be sent within ten (10) business days following the last day of the previous month and must include all the calendar days of that reportable month. The reportable month will start at 12:00 a.m. EST on the first day

		of the calendar month and end on 11:59 p.m. EST on the last day of the calendar month. For all reports, if Securus Monitoring failed to meet any System Availability requirement during the reporting period, the submitted report will have a detailed description of the issue, known cause of the issue, length of time in minutes of the issue and the corrective action Securus Monitoring took to ensure System Availability expectations are met.
14.0	For this Category of Need, provide a detailed delivery and shipping plan that can be offered to any Participating Entity. Describe how proposer will fill orders and ship Products and, specify timeframes, and include logistical capabilities that allow proposer to meet urgent requests. Ensure proposer notes any circumstances in Participating Entity location and/or Product User location that may result in delays and/or prolonged timeframes for Product delivery and/or Service issues.	Securus Monitoring's standard shipping policy is to process and ship orders to our customers within 24 hours of receipt Monday through Friday, 8 a.m. to 3 p.m. Central Time (CT), except holidays. We use an international third-party shipping vendor for all our shipping and use the two-day air delivery option. We can ship equipment via next business day delivery in emergency situations. We will maintain all equipment in proper working order. We provide a lifetime warranty against manufacturer defects. This means if any piece of Securus Monitoring-provided equipment does not function as expected, the Participating Entity's supervising officer returns it to our Houston, Texas, headquarters for testing and evaluation. We ship a replacement device to the Participating Entity until the testing and evaluation process on the returned device is completed and update the on-site inventory to keep the Participating Entity always stocked. As the original equipment manufacturer, Securus Monitoring maintains sufficient inventory of all hardware, including the consumables, in cases of emergency fulfillment. Additionally, Securus Monitoring maintains a disaster recovery plan with procedures to ensure our manufacturing, shipping, and monitoring center operations are quickly and safely moved out of the area to avoid interruptions in our services. We put these plans into action in 2017 when a hurricane hit the Houston, TX area

		leaving many parts of the city without power as well as serious flooding impacting many homes and businesses. We also deployed our disaster recovery plan in 2021 during a rare Winter storm in Houston, as well as utilizing remote operations during the COVID-19 pandemic, with no degradation to customers. In cases where there could be extensive power outages due to natural disasters at the Participating Entity or Product User locations, Securus Monitoring may provide temporary options for mobile charging and mobile applications to ensure uninterrupted monitoring.
--	--	---

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 3.0 Product Specifications

1.0

Product Specifications:

Proposer shall only propose new equipment that has been properly registered and certified under the Federal Communication Commission ("FCC") rules and regulations, as applicable. All equipment must be new, clean, damage free, and in operative order. Remanufactured or refurbished devices are not permitted under the resulting Master Agreement. Furthermore, the proposer shall identify all anticipated products, technologies, services scheduled for discontinuation and/or scheduled end-of-life that are anticipated during the initial term of the Master Agreement.

Proposer shall ensure all Products and Services proposed incorporate best-in class functionality related to charging capabilities, connectivity flexibility (not just Wi-Fi), tampering resistance, Product User fit and feel, and water resistance. Proposer shall provide Product and Service upgrades as they become available at no additional charge to the Purchasing Entity.

Per including but not limited to; the standards set by the Federal Department of Justice on electronic surveillance and/or monitoring, all Products and Services proposed under this RFP shall meet the following requirements:

1. Operate in active, passive and hybrid modes.
2. Be capable of being worn on the Product User's ankle.

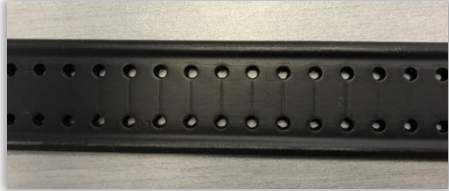
BLUtag is Securus Monitoring's small, lightweight, one-piece GPS monitoring device. The device is attached to the offender's ankle and not removed for any reason – not even to charge the battery or transmit monitoring data. While BLUtag devices operate in Active mode, if the Agency requires Hybrid or Passive modes, this device feature can be activated through VeriTracks and does not require a separate device.



BLUtag is the original one-piece GPS monitoring device

Devices can pair with BLUhome (optional) for landline reporting of monitoring data when individuals live in areas with insufficient cellular phone service. It can also pair with BLUbox (optional) for confirmation of home location when individuals live in areas impairing BLUtag's ability to receive GPS signals. While BLUtag does not require a base station, if a customer chooses to add either BLUbox or BLUhome receivers to support their radio frequency needs, the device can be matched by field personnel. More information about our optional home-based receivers (no additional charge) is provided below.

Government agencies have been using this FCC-certified device longer than any other one-piece GPS monitoring device. Since BLUtag's first deployment in early 2005,

3. Be lightweight and small. 4. Be sealed and water resistant. 5. Be hypoallergenic and must not pose a safety risk or hazard to the Product User wearing the unit or to Participating Entity personnel. 6. Be easily attached to and removed from the Product User by Participating Entity personnel in less than ten (10) minutes. 7. Be durable and shock-proof. 8. Connect to the proposer's server(s) through a cellular network. 9. Be configurable to utilize multiple cellular towers within the Participating Entity for optimum Product User location tracking. 10. Recognize wi-fi availability and roaming on cellular networks other than that of the primary cellular service provider. 11. Be supplied with a rechargeable battery that operates on standard 110-volt household current and can maintain a charge for a minimum of 16 hours. 12. Be supplied with the functionality for Participating Entity personnel to communicate with the Product User through the Product and/or Service which may include but may not be limited to; by voice, text, tone, vibration, light emitting diode, liquid crystal display.) 13. Be supplied with a backup location system in the event a GPS signal is not present. 14. Accurately restrict a Product User to the geofenced area(s) established by the Participating Entity which may include but not be limited to a range of 35 to 150 linear feet of the Product User's home and/or residence and be able to report the location of a Product User outside any structure and/or building.	Securus Monitoring has upgraded the device and expanded its functionality. Currently in its eighth generation, BLUtag reports monitoring data to VeriTracks, our secure web-based monitoring application, using nationwide cellular service. DESIGN Strap: BLUtag is designed to attach around the ankle of an offender utilizing a strap made of hypoallergenic, industrial-grade thermoplastic rubber and lined with <u>dual</u> fiber optic cables. BLUtag has a light that pulses every second to ensure there is no delay in alert due to tampering and to ensure all suspected tampers are reported. If the offender cuts or stretches the strap, the fiber optic's circuit breaks and BLUtag immediately generates and reports a strap tamper violation. Visual inspection may also indicate tampering, such as marks and cuts on the strap and/or the strap is misshapen. There is no metal or steel in the strap that would cause injury to either the offender or field personnel. Independent laboratory testing has concluded that the strap is safe for use and a copy of that testing can be supplied upon request.  Case: BLUtag's electrical components are enclosed within a case made of hypoallergenic, waterproof, industrial-grade plastic, which is waterproof up to 50 feet, as well as shock and vibration resistant. Since the case is made of hypoallergenic plastic, there is no risk of infection to the offender. There are no field operable hinges, seals, or screws. Measuring approximately 2.5" x 2.5" x 1.24" and weighing 5.27 ounces, it is lightweight and easily covered. If the offender tries to crack or break open the device case, light hits an internal sensor and triggers a tamper alert.
--	--

15. Accurately track time on an internal clock that is automatically set with periodic time checking to verify accuracy.

16. Collect and store GPS location points at a frequency not less than once every minute.

Describe how proposer will meet these requirements.

Battery: BLUtag has a lithium-ion battery that will maintain a charge for 50+ hours in between charges, which is one of the longest battery lives for a GPS monitoring device receiving one GPS location point per minute. As the device's battery power depletes, BLUtag will vibrate to notify the offender approximately 10 hours prior to losing all power. It will continue to vibrate once every 10 minutes until the battery is recharged or depleted of all power. If, after six (6) hours, the offender has not responded to notifications to recharge the battery, BLUtag will report a critical battery notification to VeriTracks. With 30 minutes of power remaining, BLUtag will report a dead battery to VeriTracks and prepares itself to go into a safe shutdown mode. If BLUtag's battery loses all power, it can be charged back to a full charge status within two (2) hours.

BLUtag contains an internal surge protector for additional protection.



BLUtag Wired Charger

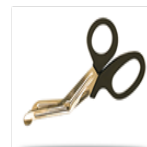
Each BLUtag device is shipped with a Wired Charger at no additional cost. Using the wired charger gives individuals the convenience of being able to charge their device wherever a standard 110-volt electrical outlet is available. To use, participants do not need to remove their device – they simply slip the charging cup onto the bottom of their BLUtag and plug the other end into the electrical outlet.

When the charging cup is attached correctly and plugged into a wall outlet, a single LED at the top of the device will:

	• Blink and then glow RED to indicate the battery had no charge remaining and is now charging, or; • Blink and then glow YELLOW to indicate the battery had some remaining charge and is now charging. • Once fully charged, a single LED will glow GREEN. Battery Replacement: BLUtag's battery has an operational life of 24 months. The battery is sealed in the case at the manufacturing facility and breaking open the case to change the batteries would cause a tamper alert. Therefore, replacement batteries are not provided as this process is completed by trained technicians in our manufacturing facilities. However, through regular charging by the offender, BLUtag will continue to operate as indicated. Device: During normal operations, an Active BLUtag will obtain one (1) GPS point per minute and upload data every 10 minutes to VeriTracks. During a violation status, BLUtag will continue to obtain one (1) GPS point every minute but the data will be reported immediately to VeriTracks. Authorized personnel can also initiate Rapid Reporting while logged into VeriTracks. This function temporarily increases the rate at which BLUtag reports data to VeriTracks from once every 10 minutes to once every minute for a period of 60 minutes. While in Rapid Reporting mode, BLUtag changes the rate at which it receives GPS location points/signal to one point <u>every 15 seconds</u> instead of the standard one point every minute. This functionality is useful if a field agent is pursuing an offender(s). For passive and hybrid options, reporting can be adjusted based on Participating Entity and Product User requirements. INSTALLATION The Participating Entity is supplied with Officer Kits containing all the necessary tools and consumable hardware required for the installation, adjustment, and removal of a BLUtag device from a Product User's ankle. The consumable items are designed for one use and then are discarded. If the strap needs to be adjusted, the
--	---

device needs to be removed and a new strap should be used.

Items in the Officer Kit, provided to each Participating Entity officer regardless of the number of devices in use at no additional charge, include:



Starting at top left: BLUtag DuraStrap, BLUtag strap cutting tool, BLUtag strap-removal tool, BLUtag strap clips, and the BLUtag clip removal tool.

After initial training, most installations take less than 10 minutes for the supervising agent to complete—including the time needed to set-up a Product User in VeriTracks. Instructions for care of the device are provided to the Product User after installation.

FUNCTIONALITY

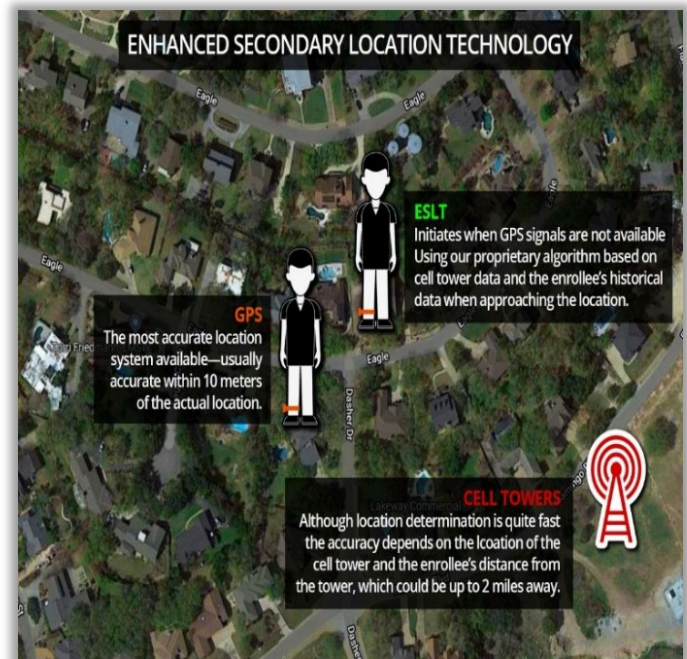
BLUtag's most used and requested functionality, includes:

- **Dual Carrier**

BLUtag is the only GPS offender monitoring device to offering simultaneous dual cellular carrier option. Securus Monitoring's EXCLUSIVE dual-carrier BLUtag

		device reduces inventory requirements and eliminates an officer's need to determine the carrier that provides the best coverage for an individual's community. This is because the BLUtag device determines the best carrier as it operates and can automatically and seamlessly switch between carriers without any impact on its reporting. Both AT&T and Verizon are within each BLUtag. By design, DualCarrier Technology offers agencies several positive, measurable impacts that include: • Supervising officers can focus on managing their caseload instead of dealing with notification headaches caused by drops in cellular network coverage. • Supervising officers can count on receiving event notifications from BLUtag in a consistent, timely manner. • BLUtag's dependable coverage means offender accountability remains more consistent. • GPS Jamming and Shielding Detection BLUtag is the <u>FIRST</u> monitoring device capable of detecting, recording and reporting when offenders deliberately jam the GPS signal and shield the device from receiving GPS signals. Jamming the GPS signal can occur from many resources but recent technological developments allow individuals to purchase low-cost, illegal electronic units to jam or interrupt the GPS signal. Shielding the BLUtag device occurs when the offender wraps the device with a foreign material that prevents the device from receiving GPS signals. Both of these events are considered tampering and violate the terms of supervision. • Enhanced Secondary Location Technology (ESLT) An offender's movements are easy to see and track in VeriTracks because BLUtag receives one GPS location point per minute. However, if the offender enters an area impairing BLUtag's ability to receive GPS location points from satellites orbiting the earth for a
--	--	---

predetermined length of time, BLUtag automatically initiates its Enhanced Secondary Location Technology. This backup tracking technology uses a combination of cellular tower data, Wi-Fi, and our proprietary algorithm to track the offender's movements. While GPS is the most accurate tracking technology, our proprietary technology places the monitored subject much closer to his/her actual movements than more traditional cellular tower-related technology, based on the distance between the offender and the cellular tower. ESLT minimizes the risks associated with limited GPS location point/signal reception.



Enhanced Secondary Location Technology uses cellular tower data and our proprietary algorithm to determine a more accurate approximation of an offender's location than traditional alternative location technologies.

- **Non-Volatile Memory**

BLUtag's on-board non-volatile memory stores up to 30 days of monitoring data. Should BLUtag lose communication with VeriTracks, it stores all monitoring data until communication is restored. Because its memory is non-volatile, BLUtag does not lose any data even if it loses power.

RELIABILITY

BLUtag monitors the compliance of enrollees with date- and time-sensitive inclusion zones, as well as exclusion zones, using GPS signals. When an offender enters an inclusion zone late or exits it prematurely, or enters an exclusion zone, BLUtag immediately detects, records, and reports the event to VeriTracks using nationwide cellular phone service. BLUtag's default programming does not notify the offender of the violation, but we can easily change the programming to meet your protocols, if required. The notification can be the flashing lights on the front of the device, or the device can vibrate or emit an audible tone, whichever is the Participating Entity's preference.

Independent tests, based on a 24-hour test period when BLUtag has an unobstructed view of the sky with ideal atmospheric conditions, confirm:

- ✓ BLUtag acquires a GPS signal within two (2) minutes;
- ✓ BLUtag obtains one (1) GPS location point per minute 99 percent of the time; and
- ✓ The GPS location points are 95 percent accurate within a range of 10 meters (33 feet).



BLUhome

- A fully integrated biometric fingerprint scanner
- GPS capabilities for additional location recognition
- 4G (LTE) cellular modem for data and voice communication
- 2.25" x 3.75" Touchscreen back-lit LCD display
- A built-in handset for two-way communication
- Adjustable RF signal range
- In the event of a power interruption, internal backup battery powers the device for up to 72 hours
- Built-in memory stores approximately 10,000 events



BLUbox

- 4.75" x 3" x 2.25", weighs 7 ounces
- Seven (7) standard/pre-set RF signal ranges (from approximately 50 to 300 feet)
- With optimal power, can all events for 10 days (with date and time stamp)
- Lithium-ion battery with operating life of 24 months

By design, BLUtag pairs with our BLUhome®, a home-based transceiver for landline reporting of monitoring data when Product Users live in areas with insufficient cellular phone service, and the BLUbox®, a home-based RF tether, to allow location verification should a Product

		User reside in a location that can impair the ability for BLUtag to consistently receive GPS signals. While BLUtag does not require a base station, if Participating Entity personnel choose to add either BLUbox or BLUhome receivers, the device can be matched by any field personnel.
--	--	---

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 4.0 Service Level Agreements and Additional Requirements for Products and Services

1.0	For this Category of Need: Service Level Agreements: Participating Entity may negotiate their own Service Level Agreements ("SLAs") per Exhibit C. At a minimum, proposer shall meet the following requirements including but not limited to: A. Exhibit C. Service Level Agreement and Maintenance and Support B. Performance Objectives Performance objectives will inform collection of data, reporting of outcome metrics, and monitoring of trends in performance. The performance metrics below are distinct from service level agreements, which are described in the scope of work. Final metrics to track proposer performance, along with the methods by which key data will be collected and reviewed, will be agreed upon through Participating Addendum between Participating Entity and awarded Contractor. Metrics may include measures to track activities conducted, efficiency, service quality, outcomes, and equity. Metrics may be reviewed by Participating Entity, or by third- party entities in partnership with Participating Entity, to monitor and audit performance, safety, and adherence to data security protocols. Participating Entity may address additional metrics in their respective Participating Addendum. Significant metrics to be collected by the awarded Contractor, reviewed by the Participating Entity, and used to evaluate the awarded proposer's performance may include:	Securus Monitoring works with each customer to develop an acceptable Service Level Agreement based on the requirements defined in Exhibit C of the Master Agreement. 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 the nature and cause of malfunctions and associated plans to avoid future errors. This information is collected by our manufacture 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 with 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 Monitoring is responsible for installation of our
-----	---	--

	1. Number of Product and/or Service malfunctions per day, week, and month, along with descriptions of the nature and cause of malfunctions and associated plans to avoid future errors. 2. Speed of proposer's resolution of malfunctions, errors, or other Product and Service maintenance requests. 3. Frequency of regular servicing and upkeep maintenance for devices, and adherence to any maintenance plan created by Participating Entities and proposer. 4. Adherence to court-ordered schedules for installation and removal of Products and Services. 5. Compliance with reporting deadlines and timelines agreed upon by Participating Entity and proposer. 6. Results of Participating Entity specific government evaluation forms documenting proposer performance. 7. Participating Entity satisfaction with training materials and presentations. 8. Participating Entity satisfaction with 24/7 help desk services at monitoring centers Describe how proposer will meet these requirements.	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 Monitoring will work with each agency to ensure compliance expectations are met. Every calendar quarter, Securus Monitoring 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 Monitoring 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.
--	---	--

2.0	Service Requests from Participating Entity and/or Product User: 1. Proposer shall respond to Product and Service request(s) from the User and Product User per the Participating Entity's Participating Addendum. 2. Product User damage as defined as Product User misuse, neglect or abuse of an installed Product and/or Service will not be covered by proposer, and proposer may bill the Purchasing Entity and/or Product User, at a fee schedule negotiated per the Participating Entity's Participating Addendum. Maintenance, Support and Servicing Agreements For Products and Services: 1. Participating Entity may negotiate and incorporate into its Participating Addendum, Product maintenance, support and/or servicing agreements for any Products and/or Services purchased outright, leased and/or rented by the Participating Entity. 2. Unless otherwise determined by the Participating Entity, pricing shall be based on a flat rate monthly fee which at a minimum includes but is not limited to; proposer time and materials, and preventative maintenance. The term of such an agreement cannot exceed the useful life of the Product(s) and/or Services rendered as determined by either the Product and/or Service manufacturer and/or the Participating Entity. Maintenance, Support and Servicing Technicians, Preventative Maintenance and Repair Parts and Service Logs: 1. Proposer shall provide an adequate quantity of maintenance, support and servicing technicians ("Service Technicians") to accommodate the diverse needs and fluctuation in volume of service requests within each	As an original equipment manufacturer, Securus Monitoring controls all aspects of manufacturing and quality assurance for all proposed equipment. Before we ship equipment, each device must pass rigorous and comprehensive testing to ensure its functionality and reliability. We certify all proposed equipment is operable, free from defect or damage and operational. The Participating Entity can reject inoperable or unacceptable equipment and return it for replacement equipment. Maintenance, Support and Servicing Agreements: 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. Should any piece of equipment require repair or replacement, authorized Participating Entity personnel retrieves the piece of equipment, exchanges it with a replacement from the Participating Entity's onsite inventory of equipment and return the original unit to our manufacturing center. When the Participating Entity needs to replenish its inventory, it places an order with our Solutions Center via email or toll-free telephone or fax. We process and ship the order within 24 hours of receipt, Monday through Friday (excluding holidays), between the hours of 8 a.m. and 3 p.m. Central Time. We absorb all maintenance, repair, and replacement costs as well as all shipping costs to and from any Participating Entity location. Lost/Stolen/Damaged Equipment When a piece of equipment is lost, stolen or damaged by a Product User and is unrecoverable, the supervising officer logs into VeriTracks and reports it as unrecoverable. When the Participating Entity needs to replace unrecoverable equipment, it places an order with our Solutions Center via email or toll-free
------------	---	--

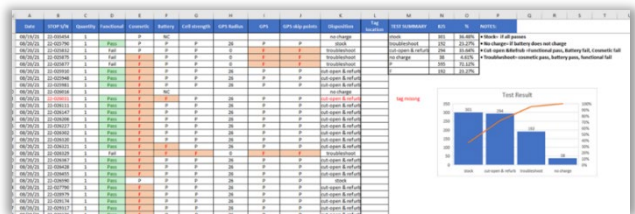
respective Participating Entity. 2. Service Technicians shall be trained by the Original Equipment Manufacturer ("OEM") and obtain and retain for the Term of the Participating Addendum, licensed and/or certified per the manufacturer. 3. Preventative Maintenance & Repair Parts, if applicable: Proposer shall: i. Perform all preventative maintenance services at the Product manufacturer's directed intervals, or as specified by a Participating Addendum. ii. Guarantee the availability of repair parts for a minimum of five (5) years after the Participating Entity's acceptance of any Product(s). iii. Ensure all Product components, spare parts, and ancillary equipment that is supplied under the Master Agreement, must conform to manufacturer specifications including for use interfacing with proposed information technology solution(s). iv. Be responsible for ensuring that any repair parts are operable and installed in accordance with manufacturer specifications. v. Ensure repair parts are new. 4. Service Logs: Proposer shall: i. Maintain a digital service log that describes any preventative maintenance and/or repair services performed by Service Technicians and track any additional information as warranted by the Participating Entity.	telephone or fax. We process and ship the order within 24 hours of receipt, Monday through Friday (excluding holidays), between the hours of 8 a.m. and 3 p.m. Central Time. Standard shipping is second day air and overnight shipping is available at no additional cost. We absorb the cost of replacement equipment if it is lost, stolen, or damaged up to the equivalent of five (5) percent of the Participating Entity's annual active equipment assigned to Product Users. For lost, stolen and/or damaged equipment exceeding five (5) percent of the Participating Entity's annual volume of active equipment assigned to Product Users, the Participating Entity reimburses Securus Monitoring for the cost of replacing unrecoverable equipment. Replacement costs for all proposed equipment are listed <i>Requirement 2: Costs</i>. Maintenance, Support and Servicing Technicians, Preventative Maintenance and Repair Parts and Service Logs: Securus Monitoring ensures that each of our technicians is trained to support and maintain each piece of equipment. We have servicing technicians across the country, with the option to utilize our reseller technicians if needed. There are no specific licensing requirements necessary. Our devices have internal programming, which regularly conducts self-tests for equipment malfunctions. The internal circuitry includes a clock that dates, and time stamps all events. The device's internal clock is synchronized through the GPS signals the device receives from the GPS satellites orbiting the earth. If it detects a malfunction, our device will immediately send a message, including date and time stamps, to VeriTracks. Securus Monitoring provides a lifetime warranty against manufacturer defects. This means if a Securus-provided device does not function as expected, the supervising officer returns it to the Securus Houston, Texas, headquarters for testing and evaluation. We will ship a new replacement device, if requested by the Participating Entity, until the testing and evaluation process on the
---	---

ii. Provide digital service log(s) and/or requested information from the Participating Entity within three (3) calendar days of written request.

returned device is completed.

We also provide a no-questions-asked return policy. The practical application of this policy means a supervising officer can return any piece of equipment at any time during the life of the contract and not give a reason for the return. The supervising officer contacts our Solutions Center to request a return shipping label. While we do not require an explanation to be given when returning a piece of equipment, if it is not functioning as expected, we would prefer the supervising officer to provide a brief explanation of the issue. This gives our Hardware Analysts a more solid starting place for testing and evaluating the equipment when it arrives. If supervising officers return the device and request a Tag Watch on it, then a complete description of the issue is required since this is a different and more comprehensive review and testing of the equipment.

All Securus Monitoring 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, and 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

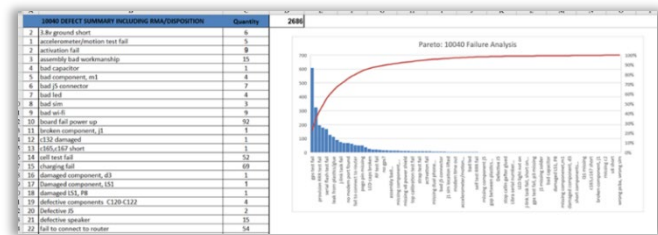


Product and Service Delivery Specifications:

1. Proposer may be required to provide a shipping quote prior to order placement from a Participating Entity.
2. Proposer must ship Product(s) within three (3) calendar days from the date of Participating Entity request, and all shipments must be Freight on Board ("FOB") Destination, unless otherwise specified by the Participating Entity.
3. Proposer must also be able to ship Product(s) overnight in emergency cases as deemed necessary by the Participating Entity and pursuant to the timeframes specified in the Participating Entity's Participating Addendum.

Monitoring Services and Requirements for Products and Services:

1. Proposer shall maintain secure central monitoring center(s) with an uninterruptible power supply, within the United States. Proposer's monitoring center(s) shall be equipped with redundant internet and telephone connectivity, as well as all other equipment required for performance of all monitoring activities required pursuant to the proposed and awarded Products and Services under the Master Agreement.
2. In order to monitor Product User activity including activities in violation as defined by each respective Participating Entity's Participating Addendum, monitoring Service(s) must be staffed and operate continuously, twenty four (24) hours per day, seven (7) days per week, and three hundred sixty five (365) days per year ("24/7/365").



Product and Service Delivery:

Securus will absorb the cost of shipping to and from the Participating Entity for the contract's life. Our standard shipping policy is to process and ship orders to customers within 24 hours of receipt Monday through Friday, 8 a.m. to 3 p.m. Central Time, except holidays. We use an international third-party shipping vendor for all our shipping and use the two-day air delivery option. We can ship equipment for next business day delivery in emergency situations.

Monitoring Services:

Securus Monitoring's dual-purpose Solutions and Monitoring Center, which is housed in our Houston, Texas, company headquarters, provides around-the-clock technical support to all customers at no additional cost. Our employees staff the Solutions Centers 24 hours a day, 365 days per year and are on duty, rather than on-call, during overnight hours, weekends, and holidays. Our Solutions Center also has bilingual staff available, and translation services available upon request.

Our Solutions Center is in a secure section of our corporate headquarters with separate biometric secure entrances and monitored security cameras. The building housing the Solutions Center has intruder detection and fire protection systems, which are monitored 24 hours a day, 365 days per year by a third-party vendor. The same security measures in Houston are also in place in our secondary Monitoring Center in Dallas, Texas. We also have an alarm permit through the City of Houston and our area is patrolled and serviced by the Houston Police department. Additionally, our Monitoring Center is under 24/7 recorded video surveillance inside and outside of this building. These cameras are monitored by our supervision staff. We have all alarm lines utilizing landlines, with a secondary back-up of cellular lines.

3. At a minimum, proposer shall perform data backup on a daily basis to prevent data loss due to power failure 4. Proposer shall provide monitoring Service(s) and indicate propose availability, scheduling, system uptimes, downtimes, and performance metrics and any other information pursuant to the Exhibit C. redline submittal. 5. Proposer's monitoring staff shall be OEM trained staff and include staff that can effectively and efficiently deliver technical assistance to the Users and Participating Entity staff and when applicable, to the Product User. i. Proposer's monitoring center operations staff must be fully trained in all proposed Products and Services including software platforms, and fulfill the requirements codified in each Participating Addendum with respect to monitoring Services. 6. Proposer shall allow unlimited access to and an unlimited number of service requests by the Participating Entity regarding Product User inquiries and/or service requests. 7. Proposer shall maintain and retain Product User data including but not limited to: term of home/residential detention, curfew, schedule modification, Product assignment and configuration, violations, Product status, and any other data sets required by the Participating Entity. 8. Proposer shall provide customizable methods and parameters of violation notification to the Users and shall accommodate changes and customization at the Participating	Additionally, our headquarters has a natural gas generator serving the Monitoring Center in the event of a power outage. If for some reason the generator is not able to function with available natural gas, we can relocate our staff to our Dallas parent headquarters. We use VoIP phones that utilize two distinct internet providers. If one provider's service is disrupted, our office automatically transitions to the secondary internet provider. Our toll-free phone number can also be redirected and answered by multiple phone systems. For example, we can point our main Monitoring Center/technical support number to either a cellular phone bridge or to our parent company's Dallas location. REAL TIME OPERATIONS VeriTracks is designed using a Live-Live operational structure, which eliminates the need to back up the monitoring data generated by our customer's programs. Live-Live means VeriTracks is always operational in two geographically separated Data Centers and "live" at both locations. The Live-Live configuration ensures system administrators are always aware of the system's health and functionality. Other vendors rely on "hot-standby" architectures where they hope the standby system comes online in a time of crisis. With a Live-Live system, the redundant system is always available and in use. Securus Monitoring's data centers are in Carrollton, Texas and Atlanta, Georgia. This configuration has many advantages. First, disaster recovery begins automatically and immediately. There is no switch to flip or any action to take. Because the backup system is always live, it is already running. Second, there is no chance the backup system will not start. Unlike a backup system that relies on a diesel generator, our Live-Live architecture is already operational and in use. Finally, restoration is easy and repeatable. The redundant chain is already scaled to handle the entire system's load. Service is not degraded as it is with the redundant systems of other vendors. STAFFING 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
---	--

Entity's request. At a minimum, methods for notification of Users and Product Users shall include immediate and next calendar day notifications via secure email, phone voice message, and cellular text message. Product User Monitoring and Activity Reports: i. Proposer shall provide digital activity reports for all Products and Services deployed by the Participating Entity. Participating Addendums will specify exact activity report content but at a minimum include, but not be limited to, the following: a. Product User missed calls and/or notifications b. Product User non-compliance with pre- determined Product User curfews c. Product User location d. Malfunctions of Product User equipment e. Product User tampering with the Product transmitter or receivers and any other components f. Detection of Product's low power or battery i. Inclusion, exclusion and zone violations upon occurrence. ii. Proposer reports shall be accessible from any web-enabled computer, and proposer shall provide login credentials for Users. Printing, and downloading of activity reports both scheduled and on-demand, should be in a standard format (Word, Excel, PDF) unless otherwise specified by the Participating Entity. iii. Proposer's proposed monitoring information technology solution must have the ability for the referring Users	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. Securus Monitoring has implemented a customer portal that allows your staff the ability to directly access all ticket information and our on-line knowledge base. All Monitoring Center technicians are Securus Monitoring associates trained at least forty (40) classroom hours and forty (40) hours of side-by-side training with an established technician before receiving their internal certification. All associates are trained in our operational procedures and those procedures are available in our online Knowledge base within our ticketing system. Upon certification, technicians can provide Monitoring Center and support services to your staff. Our Solutions Center agents are continually evaluated on their level of customer service, which is compared to the pre-defined metrics for the highest quality customer service. Agents receive more than 80 hours of training annually, which is in addition to the 80+ hours of initial training. Quarterly, each agent meets individually with the Solutions Center manager for an evaluation of the quality of customer service provided. Our primary monitoring center is in our Houston headquarters and has approximately 40 associates. Our secondary monitoring center is in Carrollton, TX, at our parent's corporate headquarters. This facility is staffed with over 300 associates, with 10 specifically trained in the basics of VeriTracks. Our 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. We allow Participating Entities an unlimited number of service requests and inquiries as we want our customers to
--	---

to enroll, terminate, modify, generate reports, add notes and otherwise perform Product User case activities by fax, email, and/or telephone.

Monitoring Service Requirements:

i. If Proposer is authorized by a Participating Entity to invoicing a Product User directly, proposer must establish in writing with the Participating Entity the fee schedule including but not limited to any late fees. Proposer must comply with any Participating Entity's directive and timeline for installing or removing Products and Services.

ii. Upon written request of the Users and/or Product User, proposer must disclose information pertaining to how Product User data is collected and utilized by the proposer and/or any subcontractor.

11. Training Requirements for Users and Product Users:

i. Proposer shall provide a web-based, on- site, and/or on-line training option(s) for both Participating Entity authorized Users and Product Users for Category of Need awarded. Proposer training materials must be available both in a digital format and upon request, paper format, unless otherwise specified by a Participating Entity.

ii. Proposer Product and Services training shall be tailored for Participating Entity authorized Users and Product Users and include but not be limited to:

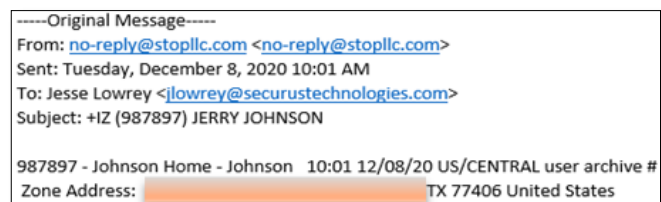
- a. Operation of the Product and/or Service including any software.
- b. Installation, deactivation,

be comfortable with our system.

The Solutions Center has three tiers of support. Tier I support resolves more than 95 percent of inquiries. If Tier I support cannot resolve the issue, the Technician elevates it to Tier II, where an analyst works with the user to answer the question. In the rare event Tier III support is needed, our hardware and/or software engineering team is brought into the loop, depending on the issue. Less than five (5) percent of inquiries need higher levels of support. In cases where remote support has not resolved a case, Securus Monitoring provides on-site technical assistance within 24 hours.

ALERTS & NOTIFICATIONS

The ability to determine when and to whom receives notifications of violations is an important component of our customer's Electronic Monitoring Programs. To better manage the offenders, VeriTracks allows authorized personnel to establish and modify violation and notification priorities and procedures based on their individual requirements. Adjusting notification methods includes using BLUtag to receive real time notifications, configure when you receive notifications directly, or to send them to a "Duty Officer" based on set time parameters (such as during holidays or vacations)



A sample of an event email notification

VeriTracks provides event and alert messages in near real time for many regularly requested options such as power failures, telephone failures, transmitter in and out of range of the field monitoring device, areas of no GPS coverage, areas of inadequate cellular coverage and violation of curfew schedules as defined for each Product User, as well as any attempts to tamper with Securus Monitoring's devices. Once data is received by VeriTracks, it will automatically send alerts for program violations via phone, text, email, and/or fax 24 hours a day, 365 days a year. If authorized personnel require the use of text messages, we provide native SMS messaging services

removal and operation of Products and Services. c. Product and Service return processes. d. Other as specified by the Participating Entity. iii. Proposer shall provide the training within ten (10) calendar days of Participating Entity's request unless otherwise specified in the Participating Addendum. iv. Upon request of the Participating Entity, proposer shall provide Participating Entity employee(s) virtual training for any new Product and Service features, at no additional charge to the Participating Entity. v. Proposer may offer additional training beyond the requirements outlined above, for a flat rate fee including per Exhibit B. Price Schedule. This fee may be negotiated by the Participating Entity and memorialized within a Participating Addendum. vi. Proposer shall provide digital user-manuals for each Product proposed under each proposer awarded Category of Need, and provide unlimited access to on-line resources, if available, at no charge to the Participating Entity. iii. At a minimum, Proposer shall provide a toll-free phone number for any technical support issue and/or service request required by a Participating Entity. Contractor shall respond to any support and/or service request within two (2) hours of Participating Entity's initial request for assistance. Participating Entity reserves the right to enact more comprehensive response times per their Participating Addendum.	that allow them to respond to the message to receive additional information or add notes to the event. REPORTING VeriTracks can produce more than 300 automatic standard reports, as well as ad hoc reports. When 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 user, a group of users, a geographic region, or the customer's entire program. VeriTracks automatically stores a copy of each generated report for future reference. Authorized personnel can print reports from the screen or export them in several common formats, including Microsoft Word and Excel, PDF, and comma delimited. Customers can restrict access to certain reports. For example, VeriTracks contains a wide variety of reports related to program management. The customer may want to restrict access to these reports to program administrators who can generate them. A Daily Summary Report is emailed to the assigned supervision staff every morning by 6:00 a.m. Central Time. This report provides a summary of all activity by Product User for the previous 24 hours. This report can be the standard report we generate to most agencies, or it can be customized with specific information required by each department. Even with customization, the report will arrive before 6:00 a.m. each morning. Upon Request, we can supply the complete list of reports available in VeriTracks. INVOICING Per diem charges begin on the day the Product User is enrolled into VeriTracks and equipment is installed on the Product User. Per diem charges end on the day the Product User is un-enrolled from VeriTracks and the equipment is removed from the enrollee. To ensure the Participating Entity's invoices reflect accurate charges for each Product User, all authorized personnel must assign equipment to a Product User in VeriTracks on the day monitoring begins and equipment must be un-assigned from a Product User
--	---

	Describe how proposer will meet these requirements.	in VeriTracks on the day monitoring ends. We generate invoices based on the enrollment/un-enrollment activity during the previous month. Our Accounts Receivables Department emails three-part invoices to the Participating Entity's designated recipient(s) for billing activity during the previous month in two formats: Adobe PDF file and Microsoft Excel spreadsheet. The first part is a summary of all the charges. The second part details the activity by office or geographic region, whichever applies to the Participating Entity's requirements. The third part provides the details behind the summaries. The details include the name of the supervising officer and the Product User, the Product User's primary and secondary IDs, the serial number of the equipment assigned to and installed on the Product User, the start date, the end date (if applicable), the total number of billing days during the billing period, and any other information that is required. If a Participating Entity requests that Securus Monitoring direct bill the Product User, that will be established at the beginning of the contract and a fee schedule will be provided. TRAINING Details about our Training Plan are provided in <i>Section 7.0: Product and Service User Training</i>.
--	--	---

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 5.0 Best Value

1.0	Explain and substantiate with data how Participating Entities are receiving best value for the proposed Products and Services under this Category of Need?	Securus Monitoring has been a leader providing electronic monitoring solutions for the better part of two (2) decades. Our hard-earned position as a leader is the result of a singular pursuit: To assist our customers in law enforcement and community corrections create of better outcomes for the communities they serve and the participants they supervise. To do so, we differentiate ourselves through the creation of true technological innovation—not imitation—and the sound and effective application of those innovations to help our customers overcome the ever-changing challenges associated with the effective management of participant populations. As proof of our innovation, Securus Monitoring (as Satellite Tracking of People LLC) has been awarded 36 patents—and counting—for our electronic monitoring solutions. Our successes have reverberated across the industry. Satellite Tracking of People was the first to introduce the one-piece GPS device—now the standard across the entire industry. Our commitment to innovation has not waned as we are the first to offer dual-carrier technology to help eliminate gaps in cellular coverage and the first to offer integrated biometric fingerprint technology in home-based RF monitoring. Here are key differentiators of our electronic monitoring equipment and services that we believe makes what we offer superior to those offered by our competitors: 1. Securus Monitoring is an original equipment manufacturer (OEM) We design, manufacture, and test ALL our electronic monitoring hardware and software. This gives us several significant advantages over our competition:
-----	---	--

		Gaps in cellular coverage can wreak havoc on an agency's ability to effectively monitor the activities of enrollees in each area. We virtually eliminate the problems caused by coverage gaps by enabling our GPS devices to automatically switch between AT&T® and Verizon® cellular networks on the fly to provide reliable, seamless coverage of enrollees as they go about their day-to-day activities. There are no switching devices, no reminders to switch networks, and no worries for supervising officers. 3. Leveraging Data GPS technology generates massive amounts of data. Securus Monitoring leads the industry in offering proprietary data analytic tools that provide you with truly meaningful insights that can help them better manage participant populations. These include: • Timeline™ - allows supervising staff a way to detect patterns or habits more easily in the locations at which a participant spends their time • Associations - provides supervising staff the ability to see in near real-time if participants <i>associate</i> (i.e., spend time) with other participants • Automated Crime Scene Correlation (ACSC) - VeriTracks receives information on reported crimes and incidents from the local law enforcement agency's records management system and the tool automatically compares the movements of participants in one community supervision program to the location of reported crimes or incidents within the same community, reporting back to supervising staff if an enrollee was near the incident location.
--	--	---

		4. Straightforward Access to Vital Data Securus Monitoring Provides Mobile Access to a Participating Entity's Data. Supervising staff operating in the field need to be provided with alert and location information for all enrollee violation in near real time. Securus Monitoring keeps this important information at their fingertips through our smartphone and tablet-enabled mobile platforms. Using a mobile device, agents can quickly and easily receive notifications, locate enrollees and process and update, and notate alert and violation notifications while in the field. Based on customer feedback, we added functionality in VeriTracks to provide a graphical representation of the frequency of locations visited by the enrollees. These are displayed in varying colors which we call Heat Maps. With these Heat Maps we can visually find patterns like frequently visited locations. 5. Enhancing Enrollee Compliance Securus Monitoring continues to introduce innovation to long-ignored "old" electronic monitoring technologies. In March 2019, Securus Monitoring introduced BLUhome, our significantly upgraded and enhanced radio frequency (RF) receiver. BLUhome has built-in technologies that help to ensure an enrollee's compliance with home confinement and agency-mandated activity schedules. The Securus Monitoring difference includes: • Biometric Fingerprint Scan Technology • Voice Communication Ability • GPS Location Confirmation • Large, Enhanced Easy-to-Read LCD Display • Rugged Design with Aerial Antennas Housed Internally
--	--	--

		6. Our Personnel The success of all projects is based on the people that will execute and support our excellent technology, is based on our team who will execute and support it. It is not an overstatement to say that Securus Monitoring has assembled a team of the most experienced and talented people in the industry.
--	--	--

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 6.0 Quality Control & Assurance Protocols and Customer Service Delivery

1.0	Quality Control/Assurance Plan: Provide a quality control/quality assurance plan that will be used for including but not limited to; the sourcing, inspection, delivery, implementation/installation maintenance, servicing, removal and disposal of proposed Products and Services under this Category of Need.	Our quality control program addresses all aspects of our monitoring system including: the design, manufacture, shipping, repair, replacement, and support of monitoring equipment; the design, implementation, integration, testing, deployment, and maintenance of monitoring software; the provision of account management, training, help desk/technical support and monitoring center services; the detection and prevention of errors; and the provision of quality assurance for the equipment and services listed in the solicitation. We evaluate and improve our quality control program continually to meet and exceed the standards of performance. A copy of our Quality Assurance Plan has been provided in Appendix A.
2.0	Customer Service Policy(ies): Provide proposer's customer service policy including those of any subcontractors that proposer will utilize under this Category of Need.	At Securus Monitoring, we are committed to providing excellent customer service to all our customers. We expect every member of our team to be committed to always providing outstanding customer service and fostering customer relationships. The following standards are the expectations of all employees. We will always: • Be polite, courteous, and professional. • Respond to customer needs in a timely manner. • Strive to improve our level of service. • Maintain accurate information on all customer accounts. • Resolve customer issues or concerns with respect and efficiency. We will never: • Fail to follow up on promised actions. • Disparage our competitors or their products. • Speak negatively about customers.

		• Engage in dishonest or morally wrong behavior. These standards have been established to ensure that Securus Monitoring delivers the highest level of customer service and value. There is a “no-tolerance” policy for failure to meet these standards.
--	--	---

Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 7.0 Product and Service User Training

1.0

For Participating Entities:

Describe proposer's training strategy inclusive of materials, delivery methodologies and scheduling relative to the proposed Products and Services under this Category of Need and differentiate between training for Product Users and Users (Participating Entity staff).

Securus Monitoring understands that effective training is critical to the success of each customer's electronic and/or alcohol monitoring program because it ensures a smooth transition, launch, and continued operations throughout the life of the program. Consequently, we work closely with each customer to develop and provide effective training for all personnel on the use of our monitoring system and all hardware and software.

There are several types of training provided to authorized representatives within each organization at **no additional charge**: initial, follow up, refresher, and new functionality. Securus will provide all training and training materials either on-site or remote, based on customer request. If training is provided on-site, the only items Securus Monitoring does not provide are a training room and a computer, laptop, or tablet with a high-speed Internet connection for each trainee. Initial training usually takes place on-site and requires a time commitment of one day to cover the use of our products (i.e., BLUtag) and the VeriTracks monitoring software functionality. We also offer new employee training if requested by a Participating Entity. When a Participating Entity requests training, we assess the total number of staff to be trained, as well as the number of locations, and provide a schedule of training with our response. We typically recommend no more than 10 people per training session but this can be adjusted based on Participating Entity requirements.

Our comprehensive initial training course covers all aspects of our monitoring system including:

- Introduction and Familiarization with products and protocols (1.5 hours): Installation/removal of electronic monitoring equipment, including

		instructions to provide offenders; Understanding customer protocols; and Officer Kit demonstration. • VeriTracks Training (4.5 hours): Enrollment/Deactivation of offenders; Creating, assigning, and editing zones and schedules; Interpreting alerts/notifications and reports; Understanding monitoring data; Determining an offender's current location; and How to report and maintain inventory. • Monitoring Center (2 hours): Testing inbound and outbound phone calls; How to return equipment and order additional devices; and Troubleshooting issues. Upon completion of the Foundations training, trainees are required to take a quiz and score at least 80% to gain access to the system. If they do not pass, they are required to also take the web-based training. Upon successfully passing the test, they are awarded a certification of completion. Our training courses take a hands-on approach, so trainees use the Securus Monitoring devices and VeriTracks to explore the features and functionality of each component and build the trainees' confidence with our monitoring system. Each trainee will receive his or her own comprehensive training guide at the beginning of the initial training. Securus Monitoring also maintains an online user manual that is accessible in VeriTracks. Online, self-paced training videos and quick reference guides on a variety of topics are available as well on a secure website, available 24 hours a day, 365 days a year. In addition to on-site and online training, our Solutions Center technicians are a great resource for field personnel if they have questions about our hardware or software. Our technicians often lead mini one-on-one training sessions using the GoToWebinar® application. This allows field officers to view the technician's monitor and see exactly how to perform a particular task. It is an
--	--	---

effective means to quickly increase an officer's knowledge.

We also provide another optional service: Proactive Customer Assistance during the first 120 contracts days, which is available at **no additional charge**. Our higher-level Solutions Center technicians review each supervising agent's Daily Summary report and looks for recurring or unusual events. If one is discovered, our technician contacts the supervising agent to discuss what may be causing it and ways to resolve it. Many times, the solution is simple: move the location of a zone, change the zone's size or shape, or edit the zone's schedule, etc. This intensive support allows agents to gain confidence with our system on an accelerated basis.



The flexibility of our training plan allows us to expand or contract any or all steps to meet our customers' needs. Our account management team has the required experience, knowledge, and skills to successfully implement/transition a program efficiently and smoothly to our monitoring system. We have done so with numerous large-scale, state-wide offender monitoring programs requiring multiple technologies.

		The team also understands the concerns and hesitations of some field personnel experience prior to and immediately after transitioning to a new software monitoring system. The entire account management team works diligently to teach, lead, and support all our customer's personnel during the early days of the launch so users quickly gain greater comfort and understanding of our system.
--	--	--

2.0	Specific to this Category of Need: Scenario: I am a Participating Entity User installing your Product. Proposer Response: 1. How will proposer train me to use the Product properly? Scenario: I am a Participating Entity User using your Services and/or proposed information technology solution. Proposer Response: How will proposer train me to use your Services and/or proposed information technology solution to full potential?	INSTALLATION By design, the installation process for our BLUtag device is a straightforward process and will not require extensive training for a Participating Entity's field personnel. The Participating Entity will be supplied with Officer Kits containing all the necessary tools and consumable hardware required for the installation, adjustment, and removal of a BLUtag device from a Product User's ankle. The consumable items are designed for one use and then are discarded. If the strap needs to be adjusted, the field officer removes the device and uses a new strap. Items in the Officer Kit, provided at no additional charge, include:  BLUtag DuraStrap™ dual fiber-optic strap  BLUtag Strap-Removal Tool  BLUtag Strap-Clips  BLUtag Clip-Removal Tool After initial training, most installations take less than 10 minutes for the supervising agent to complete—including the time needed to set-up an offender up in VeriTracks. MONITORING SOFTWARE USAGE: As noted in Section 7.0 – 1, our trainers will provide in depth training on how to use our electronic monitoring system, including software. We provide a full day of training, in addition to follow-up and refresher training as well as new feature training for product and software
-----	---	---

		releases. To ensure the Participating Entity's users are comfortable with VeriTracks, we feel that allowing users to use the system during training gets them familiar with tips, tricks, and the full dashboard. After implementation, our technicians are available to conduct mini training sessions and provide support for zone creation, enrolling Product Users, reporting, and more. As part of our transition implementation, we also provide 120 days of hands-on technical support where we review reports and alerts to find ways to help the Participating Entity best utilize the system.
--	--	--

3.0	Specific to this Category of Need: Scenario: I am a Product User using your Product and/or Service. Proposer Response: How will proposer training me to effectively use the Product and/or Service?	In addition to the Participating Entity's user training guides provided during training and online, Securus Monitoring provides pre-printed instructions for the use and care of the device to the enrollee after installation. Securus Monitoring will work with the Participating Entity's personnel to adjust these instructions to meet protocols each Participating Entity may have in place. If the Participating Entity chooses to use the optional, free of charge, enrollee mobile application, Enrollink, we will also provide instructions on how to use the application to request schedule changes, update photographs, acknowledge location requests, and communicate with Participating Entity personnel.
-----	--	--

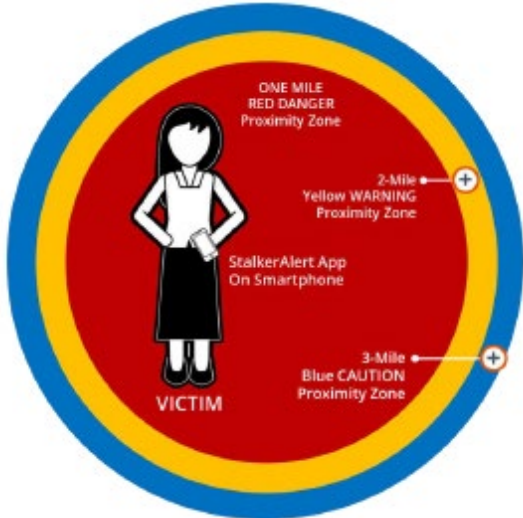
Proposer Name: Securus Monitoring, an Aventiv/Satellite Tracking of People LLC company

Category of Need: Global Positioning System Monitoring ("GPSM")

Section 8. Monitoring Services

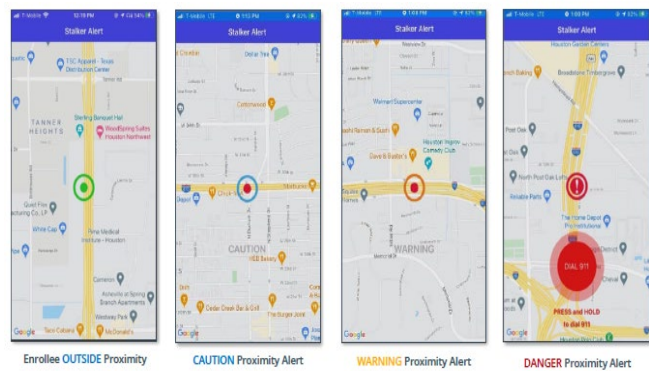
1.0	For this Category of Need, describe what steps proposer takes to detect and prevent misuse or tampering of Products and Services.	Securus Monitoring's devices have multiple methods of detecting tampering attempts with their functionality. • BLUTAG CASE Constructed of hypoallergenic, industrial-grade plastic, if the Product User tries to crack or break open the device, light hits an internal sensor and triggers a tamper alert • BLUTAG STRAP Constructed of hypoallergenic, industrial-grade thermoplastic and lined with dual fiber optic cables, if the Product User cuts or stretches the strap, the fiber optics circuit breaks and triggers a tamper alert • GPS JAMMING If the Product User utilizes an illegal electronic units designed to jam or interrupt the GPS signal, a tamper alert is triggered • GPS SHIELDING If the Product User wraps the device with a foreign material that prevents the device from receiving GPS signals a tamper alert is triggered BLUtag receives and records one GPS location point every minute and in all monitoring modes. In active mode, when the enrollee is compliant with his or her terms of supervision, BLUtag transmits data to VeriTracks at least once every 10 minutes via nationwide cellular telephone service. It immediately transmits data to VeriTracks when: a) the enrollee commits a violation (e.g., tamper violation, zone violation, etc.), b) the supervising officer initiates a Location Request (e.g., to determine the immediate location of the enrollee regardless of the last time BLUtag reported into VeriTracks) or c) the device generates an event (e.g., low battery, etc.).
-----	--	--

**Section 9 : Optional Submittal
Category 4. Value-Added Technology and Services:**

1.0	Proposer shall submit a response conforming to the requirements in this section. For each alternative solution and/or system proposed, Proposer shall provide the following: A. A detailed summary of each alternative solution and/or system proposed and its advantages to this contract portfolio. B. A detailed listing of the manufacturer(s) and model number(s) of all equipment proposed, including but not limited to detailed specifications, manuals, and the examples of how the equipment is deployed in service and/or operated. C. A detailed written summary outlining how the alternative system meets each service requirement specified in the RFP. D. A detailed written summary of how the alternative system integrates into a single reporting system. Provide a sample of the report. Proposer shall provide a comprehensive narrative and supporting proposal for all value-added technology and services proposed. Do not submit any price or cost information in this response requirement as it must be included per Exhibit B. Cost Proposal and Narrative for Category 4. Value Added	Securus Monitoring proposes the following optional value-added services: StalkerAlert Mobile Application/ StalkerAlert Device Securus Monitoring offers the StalkerAlert Mobile Application for smartphones, a powerful domestic violence prevention tool available for agencies and victims. StalkerAlert leverages the power of Securus Monitoring's proprietary VeriTracks™ electronic monitoring platform to monitor the real-time GPS locations of both the victim and offender. The application notifies the victim when the offender enters any of the three pre-designated Proximity Zones (<i>Caution, Warning, and Danger</i>). StalkerAlert PROCESS StalkerAlert creates virtual notification zones around the phone for predetermined distances:  The diagram shows a central figure labeled 'VICTIM' holding a smartphone. Three concentric circles represent proximity zones: an inner red circle labeled 'ONE MILE RED DANGER Proximity Zone', a middle yellow circle labeled '2-Mile Yellow WARNING Proximity Zone', and an outer blue circle labeled '3-Mile Blue CAUTION Proximity Zone'. A label 'StalkerAlert App On Smartphone' points to the victim's phone. Plus signs (+) are located on the yellow and blue circles. Caution Proximity Zone highlighted in BLUE (default = 3 miles)
------------	---	---

	Technology and Services submittal.	2. Warning Proximity Zone highlighted in YELLOW (default = 2 miles) 3. Danger Proximity Zone highlighted in RED (default = 1 mile) The GPS locations of the offender (via ankle worn BLUtag®) and the victim (via installed StalkerAlert Mobile App on victim's smartphone) are <u>continually</u> tracked through VeriTracks. When the offender's BLUtag device reports tracking points that occur within a Proximity Zone to VeriTracks, StalkerAlert will notify the victim by changing the highlight color around the victim's location in StalkerAlert to correspond with the current alert status. In addition, the victim will simultaneously receive an in-app notification and SMS text notification to their smartphone. PROXIMITY ALERTS Once an offender's BLUtag device has been paired with a specific victim in VeriTracks, the device will operate normally while the offender remains outside the victim's predetermined Proximity Zones. When operating normally, the BLUtag device will acquire one GPS track point every minute and report (call in) accumulated points to VeriTracks every five (5) minutes for a paired offender. Acquiring GPS tracks every minute, while in compliance with the terms of the release, will allow BLUtag to maintain 50+ hours of battery usage. While the offender remains outside their proximity zones, the victim will NOT receive any in-app notifications, nor will they receive any text notifications regarding the offender's location. In fact, the location of the offender is never displayed in the StalkerAlert Mobile Application.
--	--	---

As the offender's BLUtag reports GPS track points, increasing proximity alerts notify the victim through both an in-app notification and SMS text notification sent to the StalkerAlert Mobile Application on the victim's smartphone. Both offender and victim notifications continue to be reported in VeriTracks for Agency monitoring. In addition, the victim will have the option to **CALL 911** directly from the StalkerAlert Mobile Application screen. When the offender exits the one-mile **DANGER** proximity zone, the victim will receive an in-app notification and SMS text message confirming that the offender is no longer in that zone.



If the Participating Entity prefers a device option, Securus Monitoring offers StalkerAlert® unit, which uses GPS technology,



mobile exclusion zones, and nationwide cellular phone service to notify victims that the enrollee is in close proximity. The supervising officer installs a BLUtag device on the enrollee and assigns a StalkerAlert device to the victim, which is kept with them at all times. This allows the victim to have

		multiple layers of protective exclusion zones that travel with them at all times. The supervising officer creates mobile exclusion zones around the victim, the size of which is determined by the distance specified in the order of protection. Because the zones are stored in the offender's BLUtag and the victim's StalkerAlert, they move with the victim at all times. The mobile exclusion zone around the StalkerAlert is not tied to a physical location, therefore, the victim receives advanced warning wherever he or she goes. This allows the victim to maintain his or her daily schedule and move about freely within the community and allows the victim to create a more comprehensive and flexible safety plan. As noted in <i>Section 3: Product Specifications</i>, BLUtag detects, records, and reports the locations and movements of the Product User 24 hours a day, 365 days per year. If he/she violates the mobile exclusion zones (or any exclusion zone), StalkerAlert immediately reports the event to VeriTracks and notifies the victim by emitting an audible tone and vibrating. StalkerAlert also sends a text message notification to the victim's cellular phone. If the Product User continues to violate the zone, the victim receives additional notifications. As soon as VeriTracks receives the event notification, it sends the notification to the designated recipient(s) using email or text message. BLUtag also immediately reports the zone violation to VeriTracks since the exclusion zone information is stored in its built-in non-volatile memory. This means the designated recipient(s) receives at least two notifications on the same event – one from the Product User's BLUtag device and one from the victim's StalkerAlert unit. The supervising agent will determine which option, StalkerAlert device or StalkerAlert Mobile Application, is most practical, effective, and efficient based on each victim's circumstances.
--	--	--

		2. Solutions+ Securus Monitoring provides installation/removal services, if requested by the Participating Entity. This can include complete installation services with orientation for individuals or assisting Agency staff with this duty. With over 20 years' experience providing GPS service nationwide, our technicians can support these services on the same day of the request at any agreed upon location. Our local Solutions+ Account Manager will always be prepared to respond to enrollees, staff, or other parties' questions or provide services as needed. Our full-service option, as part of the vendor cost to install pricing, can include: • Professional Case Management - approving schedules, dispositioning of violation notifications, conducting compliance meetings, testifying in court, and providing reporting through VeriTracks • Program Administration - enrolling individuals into VeriTracks, complete installation of equipment at the Agency location, conducting orientation and providing instructions to clients, significant others, and parents, Fee Collection (if appropriate), Rebate Fee Collection (if appropriate) • On site trouble shooting of any equipment issues • Retrieval of lost equipment • Full inventory control including ordering of supplies/new equipment, cleaning of used equipment, and returns to Securus Monitoring in Houston These services are used in conjunction with our 24 hours a day, seven (7) days a week Solutions Center. Using the Solutions+ Program from Securus Monitoring is the worry-free way to get an Agency's individualized electronic monitoring program up and
--	--	--

		running on time and on budget, freeing up Agency staff to focus on the enrollees and how to best serve them during their enrollment into the program.
--	--	---

APPENDIX A: QUALITY CONTROL PLAN

Securus Monitoring is the original manufacturer of all proposed FCC-certified equipment and our manufacturing facility, based in Houston, Texas, is ISO 9001: 2015 certified. A copy of this renewal certification can be provided upon request. We continually strive to maintain quality systems and standards that allow us to continue to achieve this certification and offer a comprehensive Continuous Improvement Program, or Quality Assurance Program, that addresses all the key functional elements of this system. This program is designed to apply standardized approaches to prevent avoidable errors and proactively identify customer issues early to minimize the risk of disruption to customer activities.

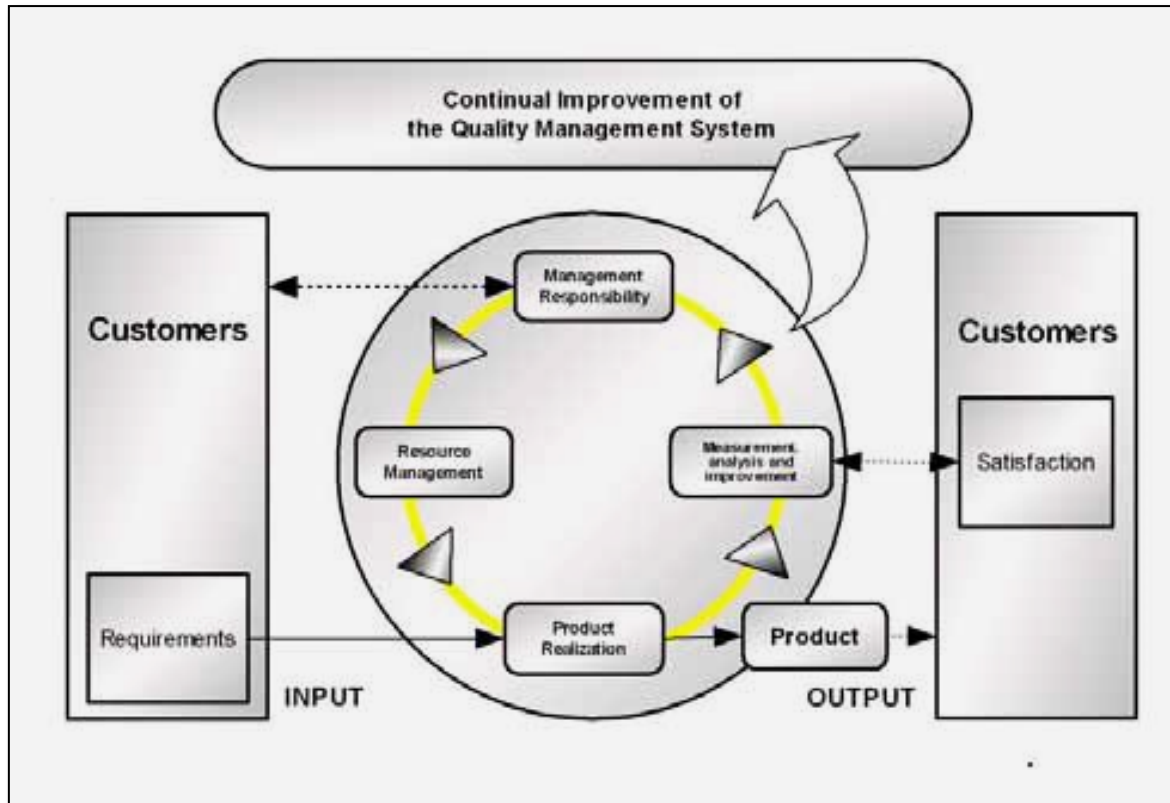
This program is segmented into three areas: (i) Product Controls ensure that hardware and software products meet customer requirements; (ii) Operational Controls ensure that customers are able to fully utilize the capabilities of the solution; and (iii) Infrastructure Controls ensure that the underlying system components function properly.

Product Controls are processes and procedures ensuring that software and hardware performance is consistent with customer requirements. Among other things, software controls include exception reporting concerning alerts, data, and other matters. Observations collected from customers through Securus Monitoring's Solutions Center or customer user group meetings as well as observations from their personnel are maintained in issue tracking software. These performance and functionality enhancements are incorporated into their system during regular quarterly releases and larger periodic upgrades. Among other things, hardware controls include equipment testing and acceptance procedures, a proactive maintenance program and incorporation of value engineering opportunities. The objective is to first avoid problems in field performance and second to critically review performance observations and incorporate improvements into Securus Monitoring's products.

Operational Controls are processes and procedures that ensure that customers can fully realize the benefits of our system. Among other things, Securus Monitoring continually monitors performance of our Solutions Center, customer implementation, and training. The Solutions Center maintains detailed contact metrics, an aging of open tickets, and coordinated support. The intent is to ensure that customer issues are addressed in a timely and complete manner. Securus Monitoring has Quality Analysts dedicated our Solutions Center that review salesforce.com cases, technician phone calls, and customer concerns. A minimum of twenty (20) customer interactions are reviewed daily and appropriate counseling sessions are conducted with the technician and the supervisor. By having both the technician and the supervisor in the review and counseling session, it further reinforces the importance of quality improvement and accurate customer communication. If technician accuracy continues to be an issue, further training and progressive discipline is implemented.

Securus Monitoring's Customer Implementation Process is a specific set of implementation steps coordinating all resources within Securus Monitoring and the customer. This process ensures that no action is missed, and new customers are activated in a smooth and orderly manner. The Training Department continually evaluates course curriculum to meet customer needs. This evaluation process has resulted in the creation of new courses and a scheduled, web-based class offering, which customers can utilize as needed.

Infrastructure Controls are processes and procedures designed to ensure the proper functioning of the underlying technology. Securus has implemented network operations center software to continually monitor key performance measures for signs of disruption. This approach includes a “Red, Yellow, Green-Light” approach to automatically alert their personnel of possible problems immediately. This frequently allows them to avoid problems without any impact on customer operations. In the event service is disrupted by internal or external factors, their personnel have already been working on the problem and customer disruption is minimized.



The following tables describe the steps taken, purpose, and frequency for each segment.

PRODUCT CONTROLS

Hardware Controls	Description	Purpose	Frequency
Equipment Manufacturing	Securus' Houston assembly component is ISO 9001:2015 certified.	Provides internationally recognized standards for quality assurance in the assembly of the devices.	ISO 9001:2015 certification is valid for three years and was awarded in 2022.
	Employee training in ISO 9001 and Six Sigma quality assurance standards.	Employees who understand both the assembly process and the standards to which the factory adheres results in higher quality devices and fewer errors.	All new employees receive comprehensive training in all aspects of assembly and manufacturing prior to starting "on the line;" existing employees receive quality assurance refresher training bi-annually.
	Employees apply internationally recognized ISO 9001 and Six Sigma standards to the assembly process of devices.	Application of the quality assurance standards provide uniformity in the assembly/manufacturing of devices that adhere to internationally recognized quality assurance standards.	Daily.

Acceptance testing for new production devices	After assembling a device, employees complete an exhaustive series of two different inspections and tests to ensure proper operations; prior to shipping a device to a customer it undergoes a third series of operational tests.	Provides consistent high quality production standards for every device and assures that every device received by customers is fully functional.	Daily and with the assembly of every device.
	Among the key functional areas tested are battery charge, low battery alert, processing monitoring data, recognizing, and generating alerts, tampering and “pings.”	Passing key functional area tests ensure every device customers receive is fully functional.	Daily and with the assembly of every device.
	Results from devices not passing any test is detailed, retained, and compiled to determine the root cause of the issue and ultimately correct it.	As failing test data is compiled and analyzed, patterns and/or trends can be detected, which can lead to solving or removing the cause of the issue.	Failed test results are detailed with every device and compiled for analysis weekly; analysis occurs weekly.
Processing customer-returned devices	Every device received from customers is accompanied by notes, usually in the Customer Portal; that data is reviewed, and testing of the device begins; every device undergoes a series of basic diagnostic tests to ensure basic operations are functional.	Before diagnostic procedures begin, standard operational testing must be completed and the device pass, which helps maintain a timely turn-around time for returned equipment.	Technicians manage their time and resources by ensuring basic device operations are functional prior to higher level diagnostics, which can require advanced testing.

	A detailed report comprising customer notes, technician notes and test results is maintained for every returned device and analyzed for root cause(s), which may lead to changes in assembly/manufacturing or training, and in worse case scenarios, a change in vendor for the electronic component.	Through the analysis of returned devices, technicians can determine or narrow down the root cause(s) of the issue and begin corrective action steps to prevent the repeat of the issue; corrective action may involve several departments.	A detailed report is started and maintained for every returned device; a thorough analysis and evaluation of returned devices is completed on a weekly basis.
	Standard acceptance testing processes are completed on every returned device before it is shipped back to the customer; devices must pass all tests prior to returning to a customer.	Customers are assured any device returned for maintenance or repair is fully functional and reliable.	Every returned device is subject to Securus' standard acceptance testing prior to shipping back to a customer.
Version Control	An extensive library of procedures and protocols govern the development of every generation for a device.	Procedures and protocols standardize the next generation process for a device, which assures customers receive the highest quality devices that are 100 percent functional and reliable.	The next generation of a device begins approximately 12 months prior to it entering the production and customer usage stages.
	Next generation testing includes device functionality and its interfacing with VeriTracks.	The next generation device must provide customers with enhanced or new functionality but must also maintain an easy and smooth interface with VeriTracks.	Periodically.

	Approximately 30 days prior to the release of the next generation device, customers receive complete information regarding functionality and interfacing with VeriTracks receive complete information regarding functionality and interfacing with VeriTracks.	Customers will consistently monitor participant with the most current and thoroughly tested next generation of a device.	Periodically.
--	--	--	---------------

Software Controls	Description	Purpose	Frequency
Software Development	An extensive library of procedures and protocols govern the development of software enhancements and new functionality.	Procedures and protocols standardize the development of enhanced and new functionality of software, which assures customers receive the highest quality software that is 100 percent functional and reliable.	Enhanced and new software functionality launches approximately once every quarter.

	Enhanced and new functionality ideas are generated through customer feedback and employees.	Developing and implementing enhanced and new functionality demonstrates responsiveness to a customer's evolving needs and expectations.	Customers provide feedback almost daily and in a variety of methods, such as discussions with the Solutions Center agents and the account management team, on-site meetings, and the exhibit hall at industry conferences and trade shows.
	All functionality ideas are added to a repository of ranked projects, and each has a brief scope of work attached to help with its priority ranking; the scope of work includes an overview of needed resources to develop and implement the idea, a calendar of major milestones, potential for expanding the new idea's functionality and benefit to the customer.	The repository of functionality ideas has four levels: able to develop and implement in 90 days or less, six months or less, 12 months or less and technologically not feasible.	The repository of functionality ideas is reviewed monthly, and each is analyzed for feasibility and needed resources. Engineers and technicians add to and expand the functionality of VeriTracks as projects are completed.
	When functionality ideas transition from the repository to active projects, the scope of work expands significantly to include a multitude of details, such as stages of development, resources, schedule of milestones, testing protocols, possible functionality conflicts or security breaches, selected customer(s) for field/trial tests and quality assurance procedures.	An expanded scope of work gives all parties details of the project and selected customer(s) can receive advanced notice of potential field/trial participation.	Periodically.

	Customers are directly involved in the production testing of enhanced and new software functionality and provide invaluable feedback regarding the level of user- friendliness, usefulness of the functionality, suggestions, and constructive criticisms for improvements.	Enhanced and new software functionality occurs because of customer's evolving needs and expectations; providing such demonstrates Securus' commitment to meeting and exceeding the customer's needs.	Customers are routinely involved in the testing and trial phase of enhanced and new software functionality.
Software Testing	A standard approach to testing is utilized; based upon the Agile Methodology used for software development. The proposed approach will follow the agreed model, which identifies both the testing stages and the deliverables that must be tested at each stage of the project lifecycle.	QA involvement during various phases of software development helps to ensure requirements are cover and the system is functioning as expected and per requirements.	Enhanced and new software functionality launches approximately once every quarter.
New Product Development & Enhancements	Description	Purpose	Frequency
	New monitoring products and enhancements of existing devices are needed to better meet the needs and expectations of customers.	The use of technology in community corrections continually changes and Securus is committed to developing and deploying the highest quality and most technologically advanced monitoring equipment.	New products are developed based on a variety of needs.

	New product ideas and needs come to the forefront based on trends in RFP requirements, meetings with clients, information from the sales staff and competitor offerings.	All ideas for new products are analyzed for feasibility and the greatest number of customers served by them.	New products are developed on an as-needed basis.
	All new product ideas are added to a repository of ranked projects and each has a brief scope of work attached to help with its priority ranking; the scope of work includes an overview of needed resources to develop and implement the idea, a calendar of major milestones, potential for expanding the new idea's functionality and benefit to the customer.	The repository of new product ideas has four levels: able to develop and implement in 90 days or less, six months or less, 12 months or less and technologically not feasible.	The repository of new product ideas is reviewed monthly and each is analyzed for feasibility and needed resources. Engineers and technicians add to and expand the functionality of the "BLUtag" product family as projects are completed.
	When a new product idea transitions from the repository to an active project, the scope of work expands significantly to include a multitude of details, such as stages of development, resources, schedule of milestones, testing protocols, possible functionality conflicts or security breaches, selected customer(s) for field/trial tests and quality assurance procedures.	An expanded scope of work gives all parties details of the project and selected customer(s) can receive advanced notice of potential field/trial participation.	Periodically.

OPERATIONAL CONTROLS

Solutions Center	Description	Purpose	Frequency
Ticket Management	Every phone call, fax and email received into the Solutions Center automatically generates a ticket, which is the Center's tracking and analysis system; even callers who hang up before speaking to Solutions Center agent is recorded and analyzed for improving the quality of the Solutions Center.	Creating a record of every phone call, fax and email allows the Solutions Center manager to detect trends, patterns, and possible issues that other departments need to address.	A ticket is automatically opened with every phone call (completed or not), fax and email every day.
	Solutions Center agents are trained to make sure all customer questions or concerns are fully addressed prior to closing a ticket. Detailed procedures highlight the steps an agent must take prior to closing a ticket. When tickets are not closed within 24 hours or less, it triggers a yellow flag to the Solutions Center manager for investigation.	Closing tickets quickly is not the goal of the ticketing system, rather the goal is for the customer to experience high level of satisfaction with the service he or she received and the information provided.	The Solutions Center manager receives an open ticket report every morning. Any open tickets are investigated and, if necessary, moved up the next level of technical customer service, Tier II.

	The Solutions Center manager analyzes all phone calls received (completed or not), fax and email for patterns and trends and submits a metrics report to the VP, Operations and COO; metrics are pre-defined and available for update to ensure customers receive the highest quality service.	The daily metrics report is both a historic document for recurring issues and comparison of the quality of the last 24 hours to the pre-defined metrics, as well as a proactive approach to curbing potential issues before they become wide-spread.	The Solutions Center manager submits the daily metrics report to the VP, Operations and COO every morning; it covers activity for the preceding 24 hours.
	The daily metrics reports are aggregated and analyzed for opportunities to better serve customers.	Providing customers with high quality, reliable and accurate service is a highly desirable in any industry; customers value good service coupled with forthright and timely answers.	The daily metrics reports are analyzed on a monthly basis and all improved service opportunities are incorporated into the following month's Solutions Center agent training.
Coordination of Tier II Support	Technical customer support is available at two levels: Tier I and Tier II. All phone calls, faxes and emails received begin at the Tier I support level. When a Tier I Solutions Center agent has been unable to resolve a Customer's issue, the ticket is passed up to a Tier II technician/engineer. All unresolved issues are automatically elevated to Tier II support.	In order to provide accurate information and a timely response to a customer's inquiry, Tier II technical support is called on where highly skilled and trained Technicians and engineers converse with the customer. Tier II support talks directly with the customer in addition to reviewing the open ticket and its notes.	Less than 5 percent of all phone calls, faxes and emails received are elevated to Tier II support.

Ongoing Solutions Center Agent Training	Solutions Center agents must receive extensive training on all hardware and software, including enhanced and new functionality.	Solutions Center agents must possess fluent knowledge of Tier I functionality of all hardware and software.	Prior to the launch of any hardware or software enhancements, the Solutions Center agents receive a thorough training on the subject matter.
	Solutions Center agents are continually evaluated on their level of customer service, which is compared to the pre- defined metrics for the highest quality customer service. Agents receive in excess of 80 hours of training annually, which is in addition to the 80+ hours of initial training. Each agent meets individually with the Solutions Center manager for an evaluation of the quality of customer service provided.	Ensuring that customer's experience a high level of satisfaction in the service they receive and the information provided are the goals of the Solutions Center.	Formalized group training on customer service occurs four times a year and on an individual basis at least once per month.
	Solutions Center agents are provided a series of talking points for the more common questions asked. The talking points meet the pre-defined customer service metrics.	Use of the talking points helps ensure that customers receive the highest level of service in a prompt, courteous and professional manner.	Talking points are reviewed and updated at least once every 90 days.

Customer Activity	Monitoring data is analyzed for potential issues, including violations, enrollment process and user accounts. The data is compared with recurring ticket topics received in the Solutions Center.	Through the comparison of data from two different sources, technicians and engineers can determine if an issue exists or may develop. This is a proactive approach to maintaining a high quality, dependable monitoring system.	Comparing monitoring data with Solutions Center tickets occurs on a daily basis. The comparison covers the previous 24-hour period of time.
Training	Every user receives a comprehensive, hands-on training about the hardware and software comprising Securus' monitoring system. Users receive training prior to the start of a new monitoring program, periodic refresher courses and prior to the launch of new or enhanced hardware and software.	Training is essential to the successful implementation and continued operation of a GPS participant monitoring program. It is one area for which Securus will not create shortcuts or lessen the amount of content or the frequency of courses.	Training is provided to all designated users prior to the beginning of starting a new GPS monitoring program, periodically during the life of the contract refresher courses are provided and prior to the launch of new or enhanced hardware and software.
	During initial training, all users receive a comprehensive and professionally developed curriculum guide/notebook. The initial training provides the foundation on which knowledge of the system's operation is built. Users receive a bound copy of the User's Manual at the end of the initial training course.	All users have access to at least three reference sources: the initial training curriculum guide/notebook, the bound User's Manual, and an online version of the User's Manual. This is in addition to the technical support provided through the Solutions Center.	Periodically.

	At the end of every training session, users are given an evaluation survey to determine the effectiveness of the trainer. All comments and suggestions are evaluated and, when possible, integrated into the trainer's presentation.	Trainer evaluation surveys are offered at the end of every course, whether it was an online or in-person class.	The VP, Operations and the Training manager meet at least twice a month to review training evaluations and develop ideas for integrated the suggestions and criticisms over the presentation.
	Through the analysis and evaluation of phone calls, faxes and emails to the Solutions Center, patterns and trends emerge that may indicate the source of the issue requires a change in training. The Solutions Center manager works closely with the Training manager to refine the training courses to address any recurring questions Solutions Center agents receive.	Training is a critical component to the successful launch and continued operation of any GPS monitoring program. As such, training is an area that requires continual evaluation and refinement to ensure recurring issues are addressed so they do not grow in scope or size.	Analysis of phone calls, faxes, and emails to the Solutions Center occurs on a daily basis. The Solutions Center manager and Training manager meet at least twice a week to discuss any patterns or trends noted in the types of questions received by Solutions Center agents.
	Training courses are offered at the convenience of the customer. Courses are provided at the customer's preferred location, a Securus facility or online.	On-site training courses are scheduled in advance and each customer promotes the offering internally. The training manager develops a schedule of online training courses and promotes them to all users. Some courses may be available on a self-directed basis.	Periodically.

New Monitoring Program Implementation	Description	Purpose	Frequency
Formal Implementation Planning and Standard Operations Communications	Before a new monitoring program begins with either a new or existing customer, an extensive meeting between Securus and the program manager(s) occurs. The comprehensive meeting covers many aspects of the program, including: • Current customer operations and the integration of Securus' services • Reports (content, frequency, etc.) • Equipment shipping logistics (initial shipment quantity, location(s), security and environment of location(s), repairs/spares, etc.) • Staff training (dates, location(s), number of user guides given at each training site, follow- up training if necessary, etc.) • Standing meetings/ conference calls (attendees, frequency, etc.)	The initial meeting between Securus and a customer prior to the launch of a new monitoring program increases the understanding and expectations between parties. It is a lengthy meeting due to the comprehensive nature of it. Not all issues are resolved, or decisions made during this meeting. It is common for a follow up meeting to occur shortly after the first one.	In-person meetings, conference calls and daily individual conversations occur throughout the implementation phase and the first 60-90 days after the launch of the monitoring program. Once the program enters standard operations, the frequency of in-person meetings, conference calls and individual conversations are reduced. The director of Customer Relations maintains regular and routine communication with all program managers to ensure a high level of satisfaction with the hardware, software, and customer service.

Inventory Control	Description	Purpose	Frequency
	Controlling a customer's inventory is critical to containing costs associated with a GPS monitoring program. Regardless of the party responsible for the cost of damaged or lost units, a program experiencing an out of the ordinary percentage of damage/loss hardware is vulnerable. Key issues for inventory control are the level of security available at the customer's location(s) for on- site inventory, and how to access the on-site inventory.	To reduce the opportunity for lost hardware, Securus recommends an individual, or a group consisting of no more than three individuals, access and control the customer's on-site inventory. This reduces the opportunity for the customer's on-site inventory to be completely depleted and for the loss of units.	Weekly
	When customers anticipate needing a higher-than-normal on-site inventory, Securus will increase its hardware production rate to meet the need. Once the extenuating circumstance has passed, the customer's standard on-site inventory level will resume.	Securus' production rate for hardware meets the usage rate for its customers. When given notice of any possible surges in use, Securus increases the production rate to meet the increased need.	Continually

INFRASTRUCTURE CONTROLS

Automated Alerts	Description	Purpose	Frequency
Health Monitor	The health of VeriTracks is monitored by the application itself and an outside program. Both quickly alerts Solutions Center technicians when an issue has developed or can potentially develop. The outside monitoring program follows a red light/yellow light notification process to rank the priority of the alert.	VeriTracks must remain healthy at all times. The dual health monitoring system provides a proactive method to quickly contain an issue or address potential ones.	Monitoring the health of VeriTracks occurs on a continuous basis.

Scheduled Maintenance	Description	Purpose	Frequency
	Proactive maintenance is scheduled for the entire GPS monitoring system.	To maintain the highest levels of health, operations and security, the entire monitoring system undergoes	The proactive maintenance program takes place once every 60 days.

Redundancy	Description	Purpose	Frequency
	The entire monitoring system is backed up with a concurrently running system on-site and at a different geographic location. These backup systems receive the same maintenance and security enhancements as the primary system. Enhancements to the backup systems occur at the same time as with the primary system.	On-site and geographical redundancy significantly reduces the chance of the system becoming inoperable or inaccessible for any length of time.	Continually.

Security	Description	Purpose	Frequency
	The data received and stored within the monitoring system is extremely sensitive and must be protected from theft or destruction. The system has built in electronic and physical security measures. As proven security measures emerge, Securus integrates them into the existing ones. Or when necessary, replaces existing electronic or physical security measures with newer, proven measures.	Safeguarding a customer's monitoring data is among the highest priorities for Securus. It employs the most technologically advanced and proven electronic and physical security measures available today.	Electronic and physical security enhancements are implemented as new, proven technologies become available.

APPENDIX B: TRANSITION PLAN

Securus Monitoring proposes a four-phase project management approach to your Electronic Monitoring Equipment and Services Program: Program Management, Pre-Enrollment, Enrollment, and Ongoing Operations. As a current NASPO provider, many of these phases and steps have already been implemented. We provide this information to understand our solid approach to implementation and to set expectations going forward.

Program Management Phase (5-7 days)

The Program Management Phase lasts less than a week, yet it is the phase we consider the most important as it lays the foundation for building a true partnership with the agencies intending to utilize Securus Monitoring's devices with VeriTracks. It can be an intensive time for both Securus Monitoring and the Participating Entity's personnel because of the amount of information exchanged and the wide array of decisions to be made.

Immediately after contract award, our Customer Success Manager will meet with agency staff to begin reviewing infrastructure, policies, and procedures, as well as all other aspects of their program. Our Training Manager will review the training curriculums and, if needed, customize them to meet the unique aspects of the Participating Entity's Electronic Monitoring program. The schedule for training is also established, as well as the location(s) and the amount of equipment to be shipped to the location(s).

Together, all parties establish system settings, level of access for various classifications of the individual county's personnel and monitoring protocols for the Participating Entity's database in VeriTracks. Some of the protocols might be creating notification preferences for specific types of events and custom reports. While we understand each user may have different requirements, there is likely some overlap in developing the protocols.

During the last part of the Program Management Phase, we build the database in VeriTracks and create user accounts for each authorized employee. Once created, we thoroughly test the database and the user accounts to ensure proper functionality.

While we are a current vendor, Securus Monitoring can use this contract transition time to make any requested changes to the Participating Entity's VeriTracks database, including reporting and protocols.

Pre-Enrollment Phase (5-7 days)

Initial training of Participating Entity personnel takes place during the Pre-Enrollment phase. Prior to the start of training, all manuals and equipment necessary (based on information gathered during Phase 1) are delivered to the training site(s). We will confirm that all equipment is configured properly and operational and all training manuals will be provided if they have not already been provided through training.

All reporting features will be configured based on discussions with authorized personnel and the database will be finalized and tested. Securus Monitoring will demonstrate operational and administrative readiness to the Contract Administrator and other interested personnel. Once the database's functionality is confirmed, our Trainers begin on-site training of authorized personnel to understand the differences between the current system and VeriTracks. Initial training covers all aspects of the VeriTracks system, including:

- Enrolling Product Users
- Creating zones
- Understanding monitoring data
- Interpreting maps, notification, and reports
- Determining the Product User's current location
- Developing schedules/curfews
- Alert processing and response
- SMS messaging and smartphone application training
- Troubleshooting issues

The course includes significant hands-on interaction with actual hardware and software, so trainees explore the features and functionality and build their confidence with the Electronic Monitoring system. Live training is typically conducted in one 1 ½ day session for every ten (10) students.

Enrollment Phase (7-14 days)

Typically, during this phase, Securus Monitoring will assist in enrolling existing offenders. It is not uncommon for Pre-Enrollment and Enrollment Phases to run concurrently to ensure a smooth transition to the new contract. As the agencies' authorized personnel complete training, any previous software is retired and VeriTracks will go live. As many of our current NASPO partner's Product Users are already enrolled in our monitoring program, the Participating Entity will save time and money by not having to go through this phase.

Ongoing Operations (After completion of enrollment phase – End of contract life)

Once all the initial offenders have been added to Securus Monitoring's electronic monitoring system, the program will enter the Ongoing Operations Phase. This phase continues for the life of the contract.

During the first 120 days of the contract, we provide optional intensive support for County personnel with Proactive Customer Assistance. Our Tier II Solutions Centers technicians provide this value-added service by reviewing the daily summary reports to check for recurring events or unusual notifications. When a technician discovers instances of recurring events or unusual notifications, he/she contacts the supervising officer to discuss it. By making this investment in the Electronic Monitoring Program's services, we help build your confidence and comfort using our VeriTracks system with our devices at a faster rate than by simply allowing personnel to contact our Solutions Center for technical support in a reactionary manner. We believe this investment helps ensure the long-term success of Participating Entity's supervision program.

Throughout the life of the contract, your designated Customer Success Manager and the Participating Entity's program manager(s) maintain close communication. Our team makes in-person visits to meet with managers, office staff, and supervising officers to hear first-hand about any issues they have with any aspect of our system, service and/or support. We believe it is important to maintain positive relationships with the frontline supervising officers and the program administrators and managers. Both audiences are critical to a successful relationship, but each has slightly different needs and expectations. To further continue the success of this contract, Securus is available to assist in the educational efforts to inform judges, prosecuting attorneys,

defense attorneys, and law enforcement and will provide ongoing training to officers using our system at annual conferences as needed.