

SECURUS

Monitoring™

an aventiv company

**NASPO VALUEPOINT
ELECTRONIC MONITORING
STATE OF NEVADA
CATEGORY 4: VALUE ADDED
SOLICITATION NUMBER 99SWC-S3474**

FEBRUARY 26, 2026

An RFP Solution Prepared for:

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

Presented by:

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

TABLE OF CONTENTS

COVER LETTER: CATEGORY 4 VALUE ADDED SERVICES	2
OFFEROR RESPONSE WORKSHEET	5
I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS	5
II. RESPONSE TO TECHNICAL CRITERIA	6
D. Customer Satisfaction.	7
SCOPE OF WORK	24
I. Background and Definitions	24
II. General Contract Requirements. (Applies to all categories)	29
III. Information Technology Security Requirements. (Applies to all categories)	31
VII. Category 4: Value Added Services	41
EXHIBIT 1: AVENTIV NIST ATTESTATION LETTER	49

COVER LETTER: CATEGORY 4 VALUE ADDED SERVICES



February 25, 2026

State of Nevada/NASPO ValuePoint

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

Re: NASPO ValuePoint RFP – Electronic Monitoring – (Value Added Services)

Dear Chuy Ampudia and NASPO ValuePoint Evaluation Committee Members,

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

Electronic monitoring is a critical tool for agencies tasked with supervising individuals convicted of serious, sexual, violent, or other offenses deemed appropriate by Participating Entities. Securus understands the responsibility that accompanies this mission and has designed its technology, services, and operational support to meet or exceed the rigorous expectations of agencies ranging from larger statewide programs to smaller county and municipal programs.

WHAT WE OFFER

In addition to our industry primary solutions which include the **BLUtag**, **BLUband/BLUhome**, **SoberTrack** and our **VeriTracks** software, we also proudly offer a variety of Value-Added Products and Services.

- **Tough Straps:** Our steel reinforced BLUtag strap engineered to provide enhanced tamper resistance and added security for enrollees classified as highrisk offenders.
- **DuraStrap:** Our disposable strap constructed of hypoallergenic, industrial-grade thermoplastic with dual fiber-optic cables to support reliable tamper detection, designed for one-time use.
- **Wired Chargers:** Our proprietary charging solution for BLUtag devices.

Securus Monitoring

- **StalkerAlert:** Our BLUtag GPS device designed for domestic violence victims to enhance safety through realtime monitoring and alerts.
- **Mobile Chargers:** Our proprietary charging solution for BLUtag devices that offers flexible charging in the field and supports extended battery performance.
- **Multi-chargers:** Our multi-station BLUtag charging tray designed to charge up to eight devices simultaneously, streamlining installations and enhancing officer productivity.
- **Solutions+:** Our full-service turnkey electronic monitoring program support, including implementation, operations, and professional case management for agencies of all sizes.
 - **Solutions+ Services:** Professional Case Management, Program Administration, Inventory Management
 - **Solutions+ Hardware Installation and Removal:** Troubleshooting, retrieval of lost or damaged equipment, device swaps
 - **Solutions+ Client Fee Collection:** Direct client fee collection
- **Monitoring Center Services:** Real-time, 24/7 alert monitoring and notification provided by trained professionals in accordance with established service level agreements (SLAs).
- **Increased Shelf Rate:** Provide increased shelf rates for all Securus Monitoring equipment.

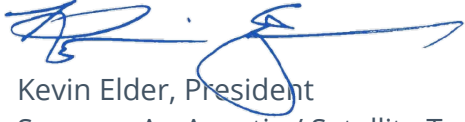
Securus is the original equipment manufacturer (OEM) of all equipment described in this proposal. We offer full-service support through our Solutions+ and Monitoring Center Services. Our ISO 9001:2015-certified assembly and manufacturing operations are based in Houston, Texas. We own, operate, maintain,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

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

We value our longstanding partnership with NASPO ValuePoint and look forward to continuing to deliver dependable cutting-edge products, responsive support, and industry

expertise that Participating Entities rely on every day. Thank you for your consideration of this proposal.

Sincerely,

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

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

OFFEROR RESPONSE WORKSHEET

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

I. RESPONSE TO MANDATORY MINIMUM REQUIREMENTS

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

II. RESPONSE TO TECHNICAL CRITERIA

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

D. CUSTOMER SATISFACTION.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

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

a. Client retention rate during the past 3 years

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

Electronic Monitoring Client Retention Rate

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

b. Customer surveys/references

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

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

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

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

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

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

Customer Name: Los Angeles County Probation/LA Pretrial Services

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

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

c. Vendor performance ratings

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

2. Provide a brief history of your company.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

In December 2013, Dallas, Texas-based Securus Technologies, Inc. acquired STOP as part of the strategy to expand its advanced technology product portfolio. Securus is the unquestioned technology leader in the law enforcement, corrections, and public safety

industries with more technology patents issued and pending than all its competitors combined. While Securus continues to operate as a wholly owned, independent subsidiary, cooperation with other Securus subsidiaries has accelerated Securus' product development and innovation in areas such as mobile applications and advanced data analytics.

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

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

SECURUS MONITORING

A brief history



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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

Goals and Purposes

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

Innovative Products

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

Understanding Our Customers' Needs

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

Unmatched Responsiveness and Service

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

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

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

Vision for the Future

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

4. Describe your company's experience performing the same or similar Scope of Work or providing the same or similar Deliverables to other public sector customers.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus, an Aventiv/Satellite Tracking of People LLC company, has been developing and marketing our GPS technologies for over 20 years. Since early 2005, we have provided government agencies and independent service providers with a proven and reliable

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

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

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

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

E. Describe what, if any, software integration support that can be provided by the Contractor to integrate with a State’s Offender Management System, if the State chooses to.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

F. Describe what, if any, artificial intelligence technologies you will be using in your performance of a Master Agreement resulting from this RFP and how and for what

purposes such technologies would be used. Include any future plans for use of AI for products and/or services.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

G. Describe the supply chain for electronic monitoring equipment. How long is the lead time to acquire equipment? Where is it shipped from. Are the products made outside of the USA?

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

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

H. Quality Assurance and Hardware Returns.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus maintains a formal **Quality Assurance (QA) and Continuous Improvement Program** designed to ensure consistent performance, reliability, and compliance across its electronic monitoring products, software, and services. This program applies standardized

controls to prevent avoidable errors, proactively identify issues, and minimize disruption to customer operations.

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

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

1. Product Controls

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

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

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

2. Operational Controls

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

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

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

3. Infrastructure Controls

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

- Continuous monitoring of data centers, systems, and network components through the Network Operations Center (NOC)
- Redundant systems and geographically diverse data centers to protect against data loss and service interruption

- Proactive analysis of system performance metrics to identify and mitigate potential issues before service is impacted

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

Ongoing Oversight and Continuous Improvement

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

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

2. Describe your return policy for hardware.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

All Securus equipment contains a bar code for tracking. When a device is returned/shipped, the bar code is scanned and recorded into our Repair Log system. This system contains all inventory, 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.

Test Result

Category	Count
stock	301
our open & refs	294
realtimehost	183
no change	18

2. List the cooperatives through which you currently have a contract, and provide sales volume information for each. Identify any restrictions on pricing and sales (e.g., most-favored nation clauses) imposed by your other cooperative contracts.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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



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

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

4. Describe features of the dedicated website you will be setting up for this Master Agreement, including, as applicable, customized price lists for each Participating Entity, staff contact information, and online ordering capabilities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

5. Describe the staff and other resources that will be allocated to your Master Agreement and the training you will provide to staff to ensure their familiarity with Master Agreement terms and pricing and their compliance therewith.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

Securus has and will continue to:

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

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

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

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

Training for Internal Staff

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

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

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

Ongoing Oversight and Compliance

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

Securus assigns dedicated contract, account management, legal, and administrative resources to its Master Agreements and provides structured training to ensure staff

understand and comply with NASPO ValuePoint terms, pricing, and participation requirements.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

7. Describe your approach to negotiation of Participating Addenda. Describe the extent to which you will provide Participating Entities flexibility in incorporating entity-specific language into their Participating Addenda. (e.g., Do you require entities to provide statutory citations for their entity-specific language? Are you able to devote resources to simultaneous negotiation of multiple Participating Addenda?)

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is prepared to provide products and services immediately upon execution of the Master Agreement and applicable Participating Addenda. Securus is the OEM for a majority of equipment proposed, this allows us to effectively support timely deployment. Our internal processes are structured to support prompt activation following contract execution, including assignment of appropriate contract management and customer support resources and coordination with Participating Entities to confirm ordering, invoicing, and implementation requirements. Once a Participating Addendum is fully executed, Securus can accept orders and begin performance in accordance with the terms of the Master Agreement and the Participating Entity's specific requirements, ensuring a timely and compliant transition to service.

9. Describe how you will ensure summary and detailed sales information is promptly, completely, and accurately reported to you by your dealers, partners, and resellers for aggregation and reporting to NASPO ValuePoint in compliance with the terms of your Master Agreement.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SCOPE OF WORK

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

I. BACKGROUND AND DEFINITIONS

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

B. All proposed tracking systems must adhere to the National Institute of Justice, Standard Offender Tracking Systems, 1004.00. All equipment (new or used) must be properly registered and certified under the Federal Communication Commission ("FCC") rules and regulations, as applicable.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

Securus (STOP) FCC Certificates

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

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

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

Certification
Issued Under the Authority of the
Federal Communications Commission

By:

TCB

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

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

Date of Grant: 12/24/2019
Application Dated: 12/23/2019

Attention: Stephen Freathy , Mr

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is
VALID ONLY for the equipment identified hereon for use under the Commission's Rules
and Regulations listed below.

FCC IDENTIFIER: S5EBTV81018

Name of Grantee: Satellite Tracking of People LLC

Equipment Class: Digital Transmission System

Notes: Ankle worn electronic tracking device

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	2412.0 - 2462.0	0.078		
	15C	2402.0 - 2480.0	0.0081		
	15C	902.3 - 914.9	0.021		

Listed output power values are from conducted measurement.

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

TCB

GRANT OF EQUIPMENT
AUTHORIZATION

Certification
Issued Under the Authority of the
Federal Communications Commission

By:

TCB

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

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

Date of Grant: 08/31/2006
Application Dated: 08/31/2006

Attention: Stephen Freathy , Mr

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for
use under the Commission's Rules and Regulations listed below.

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

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	915.0 - 915.0			

TCB

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

TCB

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

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

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

Attention: Stephen Freathy , Mr

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

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

Grant Notes

FCC Rule Parts
15C

Frequency
Range (MHz)
915.0 - 915.0

Output
Watts
0.00058

Frequency
Tolerance

Emission
Designator

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

C. Definitions:

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

Court-Requested Reporting and Chain of Custody

Securus follows forensic evidence handling procedures in that:

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

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

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

III. INFORMATION TECHNOLOGY SECURITY REQUIREMENTS. (APPLIES TO ALL CATEGORIES)

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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



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

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

Application Security

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

Network Security

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

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

Physical Security

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

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

Data Security

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

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

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

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

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

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

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

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus will contact the Purchasing Entity within 72 hours upon receipt of any electronic discovery, litigation holds, discovery searches, expert testimony, or other similar requests which in any way might reasonably require access to the Purchasing Entity's Data.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

All data centers must be based in the United States.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

B. Data Requirements

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

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

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

Network Security

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

Physical Security

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

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

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

The Securus Manufacturing Team is an equal opportunity employer and is also committed to enabling formerly incarcerated individuals to acquire employment opportunities upon release. We currently have three (3) formerly incarcerated individuals on our team that are thriving since we have given them a "second chance". We believe that good employment opportunities after incarceration reduce an individual's likelihood of returning to prison. We provide that opportunity for those job seekers that are participating in or has graduated from the PEP (Prison Entrepreneurship Program) for positions on our manufacturing team. Our second chance employees work in the return and receiving, inventory control, inspection, test departments; these roles do not have access to sensitive material or any of our secure systems within our organization and, therefore, do not affect the performance of the contract.

More information about aspects of our second chance program can be provided upon request.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus's web-based monitoring platform, **VeriTracks®**, supports **role-based access controls (RBAC)** and **access control lists (ACLs)** that allow Participating Entities to create and manage **user groups with varying access privileges**, including **read-only** and **read/write** access.

Standard User Role Types

VeriTracks user accounts are created and managed by designated program administrators and may be assigned different privilege levels based on the user's role and responsibilities. Documented user types include:

- **Restricted Users** – view only access to monitoring data and reports-only access to monitoring data and reports
- **Normal Users** – permission to create, edit, and modify data within the system
- **Administrative Users** – permission to manage users and roles, and to create and modify system data

This structure allows Participating Entities to enforce separation of duties and limit system access to only what is required for each user's function.

Granular Access and Report Restrictions

In addition to role-based permissions, VeriTracks allows agencies to **restrict access to specific reports, data sets, and features**. For example, access to certain program-level or administrative reports may be limited to designated administrators, while supervisory staff retain access only to their assigned caseloads or read-only views.

Security and Audit Support

Access to VeriTracks is limited to authorized users through secure authentication, and the system can track login attempts and selected user activities to support audit and compliance requirements. These controls ensure that access privileges are enforced and monitored in accordance with agency policy.

Securus's VeriTracks platform supports role-based access controls that allow Participating Entities to create user groups with read-only, read/write, and administrative privileges, and to restrict access to specific data and reports as needed.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

The Solution Center continuously receives and retains all data sent by each receiver and monitor together with the date and time of each occurrence via VeriTracks. All calls are recorded and available for future review. All actions taken by our technicians are recorded in VeriTracks, our secure online monitoring application.

The Reporting Tile in VeriTracks is the gateway to the reports database, which contains more than 300 reports that meet the reporting needs of our customers. VeriTracks automatically stores a copy of every generated report in case it is needed in the future. Reports can be filtered and sorted by any field and can be printed from the screen.

All data is continuously stored electronically and available online in real time. All reports are accessible by logging into VeriTracks. Reports can be printed from the screen and downloaded into numerous common formats, such as Word or Excel documents and PDF.

A full list of our available reporting can be provided upon request. However, all existing reports can be adjusted to meet any Participating Entity specific reporting need. Our report writing team can both create and customize a report, so it meets your needs and this is provided at no additional cost.

Securus has never deleted any agency data from our data center and storage devices. The data is guaranteed to be available for at least seven (7) years in an online real time format. All features and functions of VeriTracks are available for active and historical data. Although we perform off-site, off-line backups, these are for emergency circumstances and are not for everyday use or data review.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

We provide geographically redundant Data Centers, which securely house VeriTracks. Our primary Data Center is in Carrollton, Texas, and the redundant Data Center is in Atlanta, Georgia. A well-known third party operates, maintains and protects the Centers, which securely stores some of the nation's most sensitive information.

VeriTracks is designed using a Live-Live operational structure, which eliminates the need to back up the monitoring data generated by our customers' programs. Live-Live means VeriTracks is always operational in two geographically separated Data Centers and "live" at both locations. The Live-Live configuration ensures that 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.

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.

Additionally, we have the capacity and capability to provide back-up Monitoring Center services should the Participating Entity need it either in an emergency or on-going basis. We can provide this back-up service on short notice since all shifts every day of the week are staffed with live technicians.

This functionality is tested multiple times a year and to date, there have been no issues with system malfunctions.

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

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus securely stores the State's monitoring data in the State's database in VeriTracks. Our secure web-based monitoring application is housed in two geographically redundant and secure Data Centers for the life of the contract. At the end of the contract, we continue storing the State's monitoring data in our secure databases for at least seven years.

Because monitoring data is not our property, we do not proactively consider destroying any data associated with a customer's community supervision program. We do not destroy any data unless we receive written authorization containing detailed instructions from the State or a court of law. When the seventh anniversary of the contract's closing approaches, we ask the State for detailed instructions regarding the data from its community supervision programs. For juvenile participant records, we request detailed instructions from the State as the 18th birthday of the juvenile approaches.

VII. CATEGORY 4: VALUE ADDED SERVICES

Offerors may propose value added services related to Offender Electronic Monitoring. The Lead State and NASPO reserve the right not to allow additional services proposed by the Contractor in the Master Agreement.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Awards for Category 4 will not be given to Offerors who do not also qualify for an award in Category 1, 2, or 3.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Contractors awarded Category 4 may not provide Category 4 services to Purchasing Entities who are not also utilizing the Contractor's services from Category 1, 2, or 3.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

As an example:

1. Victim Notification Application
2. Case Management System
3. Offender-Paid Services
4. Smartphone Check-in and Video Call Services
5. Voice Verification Services
6. Optional Live Monitoring Services:
7. Escalating/Closed-loop Notification
8. Verbal notification made by monitoring center staff to Officer or Offender

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.

Securus is proud to offer the following Value Added Services:

- **Tough Straps:** Our steel reinforced BLUtag strap engineered to provide enhanced tamper resistance and added security for enrollees classified as highrisk offenders.
- **DuraStrap:** Our disposable strap constructed of hypoallergenic, industrial-grade thermoplastic with dual fiber-optic cables to support reliable tamper detection, designed for one-time use.

- **Wired Chargers:** Our proprietary charging solution for BLUtag devices.
- **StalkerAlert:** Our BLUtag GPS device designed for domestic violence victims to enhance safety through realtime monitoring and alerts.
- **Mobile Chargers:** Our proprietary charging solution for BLUtag devices that offers flexible charging in the field and supports extended battery performance.
- **Multi-chargers:** Our multi-station BLUtag charging tray designed to charge up to eight devices simultaneously, streamlining installations and enhancing officer productivity.
- **Solutions+:** Our full-service turnkey electronic monitoring program support, including implementation, operations, and professional case management for agencies of all sizes.
 - **Solution+ Services:** Professional Case Management, Program Administration, Inventory Management
 - **Solution+ Hardware Installation and Removal:** Troubleshooting, retrieval of lost or damaged equipment, device swaps
 - **Solution+ Client Fee Collection:** Direct client fee collection
- **Increased Shelf Rate:** Provide increased shelf rates for all Securus Monitoring equipment.

Tough Straps

- **Tough Straps®** are Securus's **enhanced, tamper resistant transmitter straps** designed for **high-risk supervision scenarios**. They are used with **BLUtag® GPS monitoring devices** to provide **additional resistance to cutting, stretching, and breakage**, while maintaining wearer safety and comfort.

Construction & Materials

- Made of **hypoallergenic, military grade thermoplastic rubber**
- Incorporates **embedded steel inserts** for added strength
- Contains **dual full-length embedded fiber-optic cables** that detect cutting or stretching
- Designed for **long-term wear** without causing irritation



Tamper Detection & Alerts

- **Cutting, stretching, or breaking** the strap interrupts the fiber-optic circuit
- Generates an **immediate Strap Tamper alert**
- Alerts are **date- and time-stamped** and reported to **VeriTracks®** via cellular communication
- Visual inspection also reveals signs of tampering (deep cuts, deformation)

Operational Characteristics

- **Disposable, single-use strap** to maintain security and hygiene
- Available in **multiple lengths** to fit a wide range of participants
- Installed using Securus-provided consumables and tools
- Designed to be **significantly more resistant** than standard thermoplastic straps

Use Cases

- High-risk or high-tamper individuals
- Programs requiring **enhanced physical security**
- Situations where additional deterrence to strap tampering is desired

DuraStrap

- **DuraStrap** is a disposable strap used with the **BLUtag® GPS device**
- Constructed of **hypoallergenic, industrial grade thermoplastic** with **dual fiberoptic cables** to support reliable tamper detection.-**grade thermoplastic-optic cables**
- Designed for **one-time use** and tool-free installation, supporting efficient field deployment and replacement.-**time use-free installation, supporting efficient field deployment and replacement.**
- Distinct from **ToughStrap**, which is a reusable, steel reinforced strap.-reinforced strap.

StalkerAlert

Securus 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 zones 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 Category 1: GPS, BLUtag detects, records, and reports the locations and movements of the enrollee 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 enrollee 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 enrollee'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.

Wired Chargers

Securus provides a **wired charging solution** for BLUtag® GPS devices as a standard component of the monitoring equipment package.

- Each BLUtag device is shipped with a Wired Charger at no additional cost **any additional chargers after the original charger will have a cost**

- The BLUtag wired charger:
 - Uses a **standard 110-volt AC wall outlet**
 - Includes a **minimum six (6)-foot power cord**
 - Allows charging **without removing the device** from the participant's ankle
 - Uses a **charging cup/cradle** that securely attaches to the bottom of the BLUtag device

Mobile Chargers

BLUtag's Mobile Charger is available for use by the Participating Entity to support any requirement for untethered charging capabilities. The Mobile Charger is a convenient way for participants to keep their BLUtag device charged and functional when extended battery life is needed. Once fully charged, the Mobile Charger can provide an **additional 24 hours of operating time** for a BLUtag device. The small size and portability of the device make it easy for participants to keep a Mobile Charger on hand for convenient use anytime, anywhere.

MOBILE CHARGERS are available at an additional cost and are used in extreme instances where there is no available power source. The Mobile Charger can recharge BLUtag adding up to an additional 24 hours.



Multi-Chargers

Securus offers **multistation charging trays** designed to support **efficient charging and device management** for electronic monitoring programs. These charging trays are part of Securus's **value added products** portfolio and are intended to **streamline field operations and improve staff productivity**.

BLUtag® Multi-Charger

- **Multistation design** that can **charge up to eight (8) BLUtag devices simultaneously**
- Designed to support **batch charging**, reducing individual handling time
- Intended for **agency facilities and field offices** to simplify daily device management
- Complements other charging options, including **standard wall chargers, vehicle chargers, and mobile chargers**



Operational Benefits

- **Improves officer efficiency** by enabling multiple devices to be charged at once
- **Reduces device turnaround time** between installations
- Supports **centralized inventory and charging workflows**
- Helps agencies maintain device readiness without issuing individual chargers for every device

Solutions+

Solutions+® is Securus's **full-service support program** designed to assume operational and administrative responsibilities for electronic monitoring programs, allowing Agencies to **reduce staff workload while maintaining full program oversight**. Solutions+ operates in coordination with Securus's 24/7 Solutions and Monitoring Center and the VeriTracks® platform.

1. Solution+ Services

When selected by a Participating Entity, Solutions+® may include:

- **Professional Case Management**
 - Approving and managing schedules
 - Dispositioning violation notifications
 - Conducting compliance meetings
 - Testifying in court (as required)
 - Generating reports through VeriTracks®

- **Program Administration**
 - Enrolling and unenrolling individuals in VeriTracks
 - Complete installation and removal of monitoring equipment
 - Conducting client orientations and providing instructions to clients and families
 - Fee collection and rebate fee collection (when applicable)
- **Inventory Management**
 - Ordering and tracking equipment and consumables
 - Cleaning, testing, and returning equipment to Securus facilities
 - Full inventory control and logistics coordination

2. Solution+ Hardware Installation and Removal

- **Field and Technical Services**
 - Onsite troubleshooting of equipment issues
 - Retrieval of lost or damaged equipment
 - Device swaps and maintenance support

3. Solution+ Client Fee Collection

- Direct client fee collection
- Minimizes agency billing and collections administration
- Secure, convenient payment options for monitored individuals

Integration With Monitoring Operations

Solutions+® services are delivered alongside Securus's **24 hours a day, 7 days a week Solutions Center**, ensuring:

- Continuous event monitoring
- Immediate response to alerts and violations
- Adherence to Agency defined protocols for escalation and notification-defined protocols for escalation and notification

Agencies retain **full visibility and control** through VeriTracks®, while Solutions+ staff execute day-to-day operational tasks on the Agency's behalf.

Program Benefits

- Reduces Agency staffing and administrative burden
- Accelerates program implementation and scalability
- Ensures consistent application of monitoring protocols
- Provides access to experienced monitoring professionals with nationwide program experience

Increased Shelf Rate

Provide increased shelf rates for all Securus Monitoring equipment.

EXHIBIT 1: AVENTIV NIST ATTESTATION LETTER



August 15, 2025

To Whom It May Concern,

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

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

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

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

Scope: IC++

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

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

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

Outcome / Disposition:

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

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

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



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

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

Thank you,

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