

**PROFESSIONAL SERVICES AGREEMENT**

**ELECTRONIC MONITORING SERVICES**

**CATEGORY 2 – GLOBAL POSITIONING SYSTEM (GPS)**

BETWEEN



COOK COUNTY GOVERNMENT

COOK COUNTY ADULT PROBATION  
COOK COUNTY JUVENILE PROBATION  
SHERIFF

AND

TRACK GROUP, INC.

CONTRACT NO. 1515-15006B  
(PURCHASE ORDER NO. 70000095333)

# **PROFESSIONAL SERVICES AGREEMENT**

## **TABLE OF CONTENTS**

TERMS AND CONDITIONS .....	1
ARTICLE 1) INCORPORATION OF BACKGROUND .....	1
ARTICLE 2) DEFINITIONS.....	1
a) Definitions .....	1
b) Interpretation .....	2
c) Incorporation of Exhibits .....	3
ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT.....	3
a) Scope of Services .....	3
b) Deliverables .....	3
c) Standard of Performance.....	4
d) Personnel .....	4
e) Minority and Women Owned Business Enterprises Commitment.....	5
f) Insurance .....	6
g) Indemnification .....	8
h) Confidentiality and Ownership of Documents .....	9
i) Patents, Copyrights and Licenses .....	9
j) Examination of Records and Audits .....	10
k) Subcontracting or Assignment of Contract or Contract Funds.....	11
ARTICLE 4) TERM OF PERFORMANCE.....	12
a) Term of Performance .....	12
b) Timeliness of Performance .....	13
c) Agreement Extension Option.....	13
ARTICLE 5) COMPENSATION .....	13
a) Basis of Payment.....	13
b) Method of Payment.....	13
c) Funding .....	14
d) Non-Appropriation.....	14
e) Taxes .....	15
f) Price Reduction.....	15
g) Consultant Credits.....	15
ARTICLE 6) DISPUTES .....	15
ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS.....	16
ARTICLE 8) SPECIAL CONDITIONS.....	16
a) Warranties and Representations.....	16
b) Ethics .....	17
c) Joint and Several Liability .....	17
d) Business Documents .....	18
e) Conflicts of Interest.....	18
f) Non-Liability of Public Officials .....	19
ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET.....	19

a)	Events of Default Defined .....	19
b)	Remedies .....	20
c)	Early Termination .....	22
d)	Suspension .....	22
e)	Right to Offset.....	23
f)	Delays .....	23
g)	Prepaid Fees .....	23
	<b>ARTICLE 10) GENERAL CONDITIONS .....</b>	<b>24</b>
a)	Entire Agreement .....	24
b)	Counterparts .....	25
c)	Contract Amendments .....	25
d)	Governing Law and Jurisdiction.....	25
e)	Severability .....	26
f)	Assigns .....	26
g)	Cooperation .....	26
h)	Waiver .....	26
i)	Independent Consultant .....	27
j)	Governmental Joint Purchasing Agreement .....	27
k)	Comparable Government Procurement.....	27
	<b>ARTICLE 11) NOTICES.....</b>	<b>28</b>
	<b>ARTICLE 12) AUTHORITY .....</b>	<b>29</b>

## **List of Exhibits**

Exhibit 1	Scope of Services
Exhibit 2	Schedule of Compensation
Exhibit 3	Minority and Women Owned Business Enterprise Commitment
Exhibit 4	Evidence of Insurance
Exhibit 5	Board Authorization
Exhibit 6	CJIS Security Policy
Exhibit 7	Cook County Information Technology Special Conditions (ITSCs)
Exhibit 8	Identification of Subcontractors/Suppliers/Subconsultant Form
Exhibit 9	Economic Disclosure Statement

## AGREEMENT

This Agreement is made and entered into by and between the County of Cook, a public body corporate of the State of Illinois, on behalf of Office of the Chief Procurement Officer hereinafter referred to as "County" and Track Group, Inc., doing business as a Corporation of the State of Illinois hereinafter referred to as "Consultant", pursuant to authorization by the Cook County Board of Commissioners on January 24, 2019, as evidenced by Board Authorization letter attached hereto as EXHIBIT "5".

## BACKGROUND

*The County of Cook issued a Request for Proposals "RFP" for Electronic Monitoring Services. Proposals were evaluated in accordance with the evaluation criteria published in the RFP. The Consultant was selected based on the proposal submitted and evaluated by the County representatives.*

*Consultant represents that it has the professional experience and expertise to provide the necessary services and further warrants that it is ready, willing and able to perform in accordance with the terms and conditions as set forth in this Agreement.*

NOW, THEREFORE, the County and Consultant agree as follows:

## TERMS AND CONDITIONS

### **ARTICLE 1) INCORPORATION OF BACKGROUND**

The Background information set forth above is incorporated by reference as if fully set forth here.

### **ARTICLE 2) DEFINITIONS**

#### a) Definitions

The following words and phrases have the following meanings for purposes of this Agreement:

**"Additional Services"** means those services which are within the general scope of Services of this Agreement, but beyond the description of services required under Article 3, and all services reasonably necessary to complete the Additional Services to the standards of performance required by this Agreement. Any Additional Services requested by the Using Agency require the approval of the Chief Procurement Officer in a written amendment to this Agreement before Consultant is obligated to perform those Additional Services and before the County becomes obligated to pay for those Additional Services.

**"Agreement"** means this Professional Services Agreement, including all exhibits attached to it and incorporated in it by reference, and all amendments, modifications or revisions made in accordance with its terms.

**"Chief Procurement Officer"** means the Chief Procurement Officer for the County of Cook and any representative duly authorized in writing to act on his behalf.

**"Services"** means, collectively, the services, duties and responsibilities described in Article 3 of this Agreement and any and all work necessary to complete them or carry them out fully and to the standard of performance required in this Agreement.

**"Subcontractor"** or **"Subconsultant"** means any person or entity with whom Consultant contracts to provide any part of the Services, of any tier, suppliers and materials providers, whether or not in privity with Consultant.

**"Using Agency"** shall mean the department of agency within Cook County including elected officials.

**b) Interpretation**

- i) The term "**include**" (in all its forms) means "include, without limitation" unless the context clearly states otherwise.
- ii) All references in this Agreement to Articles, Sections or Exhibits, unless otherwise expressed or indicated are to the Articles, Sections or Exhibits of this Agreement.
- iii) Words importing persons include firms, associations, partnerships, trusts, corporations and other legal entities, including public bodies, as well as natural persons.
- iv) Any headings preceding the text of the Articles and Sections of this Agreement, and any tables of contents or marginal notes appended to it are solely for convenience or reference and do not constitute a part of this Agreement, nor do they affect the meaning, construction or effect of this Agreement.
- v) Words importing the singular include the plural and vice versa. Words of the masculine gender include the correlative words of the feminine and neuter genders.
- vi) All references to a number of days mean calendar days, unless expressly indicated otherwise.

c) **Incorporation of Exhibits**

The following attached Exhibits are made a part of this Agreement:

Exhibit 1	Scope of Services
Exhibit 2	Schedule of Compensation
Exhibit 3	Minority and Women Owned Business Enterprise Commitment
Exhibit 4	Evidence of Insurance
Exhibit 5	Board Authorization
Exhibit 6	CJIS Security Policy
Exhibit 7	Cook County Information Technology Special Conditions (ITSCs)
Exhibit 8	Identification of Subcontractors/Suppliers/Subconsultant Form
Exhibit 9	Economic Disclosure Statement

**ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT**

a) **Scope of Services**

This description of Services is intended to be general in nature and is neither a complete description of Consultant's Services nor a limitation on the Services that Consultant is to provide under this Agreement. Consultant must provide the Services in accordance with the standards of performance set forth in Section 3c. The Services that Consultant must provide include, but are not limited to, those described in Exhibit 1, Scope of Services and Time Limits for Performance, which is attached to this Agreement and incorporated by reference as if fully set forth here.

b) **Deliverables**

In carrying out its Services, Consultant must prepare or provide to the County various Deliverables. "**Deliverables**" include work product, such as written reviews, recommendations, reports and analyses, produced by Consultant for the County.

The County may reject Deliverables that do not include relevant information or data, or do not include all documents or other materials specified in this Agreement or reasonably necessary for the purpose for which the County made this Agreement or for which the County intends to use the Deliverables. If the County determines that Consultant has failed to comply with the foregoing standards, it has 30 days from the discovery to notify Consultant of its failure. If Consultant does not correct the failure, if it is possible to do so, within 30 days after receipt of notice from the County specifying the failure, then the County, by written notice, may treat the failure as a default of this Agreement under Article 9.

Partial or incomplete Deliverables may be accepted for review only when required for a specific and well-defined purpose and when consented to in advance by the County. Such Deliverables will not be considered as satisfying the requirements of this Agreement and

partial or incomplete Deliverables in no way relieve Consultant of its commitments under this Agreement.

**c) Standard of Performance**

Consultant must perform all Services required of it under this Agreement with that degree of skill, care and diligence normally shown by a consultant performing services of a scope and purpose and magnitude comparable with the nature of the Services to be provided under this Agreement. Consultant acknowledges that it is entrusted with or has access to valuable and confidential information and records of the County and with respect to that information, Consultant agrees to be held to the standard of care of a fiduciary.

Consultant must assure that all Services that require the exercise of professional skills or judgment are accomplished by professionals qualified and competent in the applicable discipline and appropriately licensed, if required by law. Consultant must provide copies of any such licenses. Consultant remains responsible for the professional and technical accuracy of all Services or Deliverables furnished, whether by Consultant or its Subconsultants or others on its behalf. All Deliverables must be prepared in a form and content satisfactory to the Using Agency and delivered in a timely manner consistent with the requirements of this Agreement.

If Consultant fails to comply with the foregoing standards, Consultant must perform again, at its own expense, all Services required to be re-performed as a direct or indirect result of that failure. Any review, approval, acceptance or payment for any of the Services by the County does not relieve Consultant of its responsibility for the professional skill and care and technical accuracy of its Services and Deliverables. This provision in no way limits the County's rights against Consultant either under this Agreement, at law or in equity.

**d) Personnel**

**i) Adequate Staffing**

Consultant must, upon receiving a fully executed copy of this Agreement, assign and maintain during the term of this Agreement and any extension of it an adequate staff of competent personnel that is fully equipped, licensed as appropriate, available as needed, qualified and assigned exclusively to perform the Services. Consultant must include among its staff the Key Personnel and positions as identified below. The level of staffing may be revised from time to time by notice in writing from Consultant to the County and with written consent of the County, which consent the County will not withhold unreasonably. If the County fails to object to the revision within 14 days after receiving the notice, then the revision will be considered accepted by the County.

ii) **Key Personnel**

Consultant must not reassign or replace Key Personnel without the written consent of the County, which consent the County will not unreasonably withhold. "**Key Personnel**" means those job titles and the persons assigned to those positions in accordance with the provisions of this Section 3.d (ii). The Using Agency may at any time in writing notify Consultant that the County will no longer accept performance of Services under this Agreement by one or more Key Personnel listed. Upon that notice Consultant must immediately suspend the services of the key person or persons and must replace him or them in accordance with the terms of this Agreement. A list of Key Personnel is found in Exhibit 1, Scope of Services.

iii) **Salaries and Wages**

Consultant and Subconsultants must pay all salaries and wages due all employees performing Services under this Agreement unconditionally and at least once a month without deduction or rebate on any account, except only for those payroll deductions that are mandatory by law or are permitted under applicable law and regulations. If in the performance of this Agreement Consultant underpays any such salaries or wages, the Comptroller for the County may withhold, out of payments due to Consultant, an amount sufficient to pay to employees underpaid the difference between the salaries or wages required to be paid under this Agreement and the salaries or wages actually paid these employees for the total number of hours worked. The amounts withheld may be disbursed by the Comptroller for and on account of Consultant to the respective employees to whom they are due. The parties acknowledge that this Section 3.d (iii) is solely for the benefit of the County and that it does not grant any third party beneficiary rights.

e) **Minority and Women Owned Business Enterprises Commitment**

In the performance of this Agreement, including the procurement and lease of materials or equipment, Consultant must abide by the minority and women's business enterprise commitment requirements of the Cook County Ordinance, (Article IV, Section 34-267 through 272) except to the extent waived by the Compliance Director, which are set forth in Exhibit 3. Consultant's completed MBE/WBE Utilization Plan evidencing its compliance with this requirement are a part of this Agreement, in Form 1 of the MBE/WBE Utilization Plan, upon acceptance by the Compliance Director. Consultant must utilize minority and women's business enterprises at the greater of the amounts committed to by the Consultant for this Agreement in accordance with Form 1 of the MBE/WBE Utilization Plan.

f) **Insurance**

Prior to the effective date of this Contract, the Contractor, at its cost, shall secure and maintain at all times, unless specified otherwise, until completion of the term of this Contract the insurance specified below.

Nothing contained in these insurance requirements is to be construed as limiting the extent of the Contractor's responsibility for payment of damages resulting from its operations under this Contract.

Contractor shall require all Subcontractors to provide the insurance required in this Agreement, or Contractor may provide the coverages for Subcontractors. All Subcontractors are subject to the same insurance requirements as Contractor except paragraph (d) Excess Liability or as specified otherwise.

The Cook County Department of Risk Management maintains the right to modify, delete, alter or change these requirements.

**Coverages**

(a) **Workers Compensation Insurance**

Workers' Compensation shall be in accordance with the laws of the State of Illinois or any other applicable jurisdiction.

The Workers Compensation policy shall also include the following provisions:

- (1) Employers' Liability coverage with a limit of
  - \$500,000 each Accident
  - \$500,000 each Employee
  - \$500,000 Policy Limit for Disease

(b) **Commercial General Liability Insurance**

The Commercial General Liability shall be on an occurrence form basis (ISO Form CG 0001 or equivalent) to cover bodily injury, personal injury and property damage. Coverage shall have no exclusions or limitations for sexual molestation and abuse.

Each Occurrence	\$ 1,000,000
General Aggregate	\$ 2,000,000
Completed Operations Aggregate	\$ 2,000,000

The General Liability policy shall include the following coverages:

- (a) All premises and operations;

- (b) Contractual Liability;
- (c) Products/Completed Operations;
- (d) Severability of interest/separation of insureds clause

(c) **Commercial Automobile Liability Insurance**

When any vehicles are used in the performance of this contract, Contractor shall secure Automobile Liability Insurance for bodily injury and property damage arising from the Ownership, maintenance or use of owned, hired and non-owned vehicles with a limit no less than \$1,000,000 per accident.

(d) **Umbrella/Excess Liability**

Such policy shall be excess over the Commercial General Liability, Automobile Liability, and Employer's Liability with limits not less than the following amounts:

Each Occurrence:	\$1,000,000
------------------	-------------

(e) **Professional Liability**

Contractor shall secure Professional Liability insurance covering any and all claims arising out of the performance or nonperformance of professional services for the County under this Agreement. This professional liability insurance shall remain in force for the life of the Contractor's obligations under this Agreement, and shall have a limit of liability of not less than \$2,000,000 per claim. If any such policy is written on a claims-made form, the retroactive date shall be prior to the effective date of this contract. Claims made form coverage, or extended reporting following the expiration or termination of this contract, shall be maintained by the Contractor for a minimum of three years following the expiration or early termination of this contract and the Contractor shall annually provide the County with proof of renewal. Subcontractors performing professional services for the Contractor must maintain limits of not less than \$1,000,000 with the same terms in this section.

**Additional requirements**

(a) **Additional Insured**

The required insurance policies, with the exception of the Workers Compensation and Professional Liability, shall name Cook County, its officials, employees and agents as additional insureds. The Commercial General Liability policy shall be on a primary and non-contributory basis. Any insurance or self-insurance maintained by Cook County shall be excess of the Contractor's insurance and shall not

contribute with it. The full policy limits and scope of protection shall apply to Cook County as an additional insured even if they exceed the requirements specified above.

(b) **Qualification of Insurers**

All insurance companies providing coverage shall be licensed or approved by the Department of Insurance, State of Illinois, and shall have a financial rating no lower than (A-) VII as listed in A.M. Best's Key Rating Guide, current edition or interim report. Companies with ratings lower than (A-) VII will be acceptable only upon consent of the Cook County Department of Risk Management. The insurance limits required herein may be satisfied by a combination of primary, umbrella and/or excess liability insurance policies.

(c) **Insurance Notices**

Contractor shall provide the Office of the Chief Procurement Officer with sixty (60) days advance written notice in the event any required insurance will be cancelled, materially reduced or non-renewed. Contractor shall secure replacement coverage to comply with the stated insurance requirements and provide new certificates of insurance to the Office of the Chief Procurement Officer.

Prior to the date on which Contractor commences performance of its part of the work, Contractor shall furnish to the Office of the Chief Procurement Officer certificates of insurance maintained by Contractor. The receipt of any certificate of insurance does not constitute agreement by the County that the insurance requirements have been fully met or that the insurance policies indicated on the certificate of insurance are in compliance with insurance required above.

In no event shall any failure of the County to receive certificates of insurance required hereof or to demand receipt of such Certificates of Insurance be construed as a waiver of Contractor's obligations to obtain insurance pursuant to these insurance requirements.

(d) **Waiver of Subrogation Endorsements**

All insurance policies must contain a Waiver of Subrogation Endorsement in favor of Cook County.

(g) **Indemnification**

The Consultant covenants and agrees to indemnify and save harmless the County and its commissioners, officials, employees, agents and representatives, and their respective heirs, successors and assigns, from and against any and all costs, expenses, attorney's fees, losses, damages and liabilities incurred or suffered directly or indirectly from or attributable to any claims arising out of or incident to the performance or nonperformance of the Contract

by the Consultant, or the acts or omissions of the officers, agents, employees, Consultants, subconsultants, licensees or invitees of the Consultant. The Consultant expressly understands and agrees that any Performance Bond or insurance protection required of the Consultant, or otherwise provided by the Consultant, shall in no way limit the responsibility to indemnify the County as hereinabove provided.

**h) Confidentiality and Ownership of Documents**

Consultant acknowledges and agrees that information regarding this Contract is confidential and shall not be disclosed, directly, indirectly or by implication, or be used by Consultant in any way, whether during the term of this Contract or at any time thereafter, except solely as required in the course of Consultant's performance hereunder. Consultant shall comply with the applicable privacy laws and regulations affecting County and will not disclose any of County's records, materials, or other data to any third party. Consultant shall not have the right to compile and distribute statistical analyses and reports utilizing data derived from information or data obtained from County without the prior written approval of County. In the event such approval is given, any such reports published and distributed by Consultant shall be furnished to County without charge.

All documents, data, studies, reports, work product or product created as a result of the performance of the Contract (the "Documents") shall be included in the Deliverables and shall be the property of the County of Cook. It shall be a breach of this Contract for the Consultant to reproduce or use any documents, data, studies, reports, work product or product obtained from the County of Cook or any Documents created hereby, whether such reproduction or use is for Consultant's own purposes or for those of any third party. During the performance of the Contract Consultant shall be responsible of any loss or damage to the Documents while they are in Consultant's possession, and any such loss or damage shall be restored at the expense of the Consultant. The County and its designees shall be afforded full access to the Documents and the work at all times.

**i) Patents, Copyrights and Licenses**

If applicable, Consultant shall furnish the Chief Procurement Officer with all licenses required for the County to utilize any software, including firmware or middleware, provided by Consultant as part of the Deliverables. Such licenses shall be clearly marked with a reference to the number of this County Contract. Consultant shall also furnish a copy of such licenses to the Chief Procurement Officer. Unless otherwise stated in these Contract documents, such licenses shall be perpetual and shall not limit the number of persons who may utilize the software on behalf of the County.

Consultant agrees to hold harmless and indemnify the County, its officers, agents, employees and affiliates from and defend, as permitted by Illinois law, at its own expense (including reasonable attorneys', accountants' and consultants' fees), any suit or proceeding brought against County based upon a claim that the ownership and/or use of equipment, hardware and software or any part thereof provided to the County or utilized in performing Consultant's

services constitutes an infringement of any patent, copyright or license or any other property right.

In the event the use of any equipment, hardware or software or any part thereof is enjoined, Consultant with all reasonable speed and due diligence shall provide or otherwise secure for County, at the Consultant's election, one of the following: the right to continue use of the equipment, hardware or software; an equivalent system having the Specifications as provided in this Contract; or Consultant shall modify the system or its component parts so that they become non-infringing while performing in a substantially similar manner to the original system, meeting the requirements of this Contract.

**j) Examination of Records and Audits**

The Consultant agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after the final payment under the Contract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices, and records of the Consultant related to the Contract, or to Consultant's compliance with any term, condition or provision thereof. The Consultant shall be responsible for establishing and maintaining records sufficient to document the costs associated with performance under the terms of this Contract.

The Consultant further agrees that it shall include in all of its subcontracts hereunder a provision to the effect that the Subcontractor agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after final payment under the subcontract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices and records of such Subcontractor involving transactions relating to the subcontract, or to such Subcontractor compliance with any term, condition or provision thereunder or under the Contract.

In the event the Consultant receives payment under the Contract, reimbursement for which is later disallowed by the County, the Consultant shall promptly refund the disallowed amount to the County on request, or at the County's option, the County may credit the amount disallowed from the next payment due or to become due to the Consultant under any contract with the County.

To the extent this Contract pertains to Deliverables which may be reimbursable under the Medicaid or Medicare Programs, Consultant shall retain and make available upon request, for a period of four (4) years after furnishing services pursuant to this Agreement, the contract, books, documents and records which are necessary to certify the nature and extent of the costs of such services if requested by the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives.

If Consultant carries out any of its duties under the Agreement through a subcontract with a related organization involving a value of cost of \$10,000.00 or more over a 12 month period, Consultant will cause such subcontract to contain a clause to the effect that, until the expiration of four years after the furnishing of any service pursuant to said subcontract, the related organization will make available upon request of the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives, copies of said subcontract and any books, documents, records and other data of said related organization that are necessary to certify the nature and extent of such costs. This paragraph relating to the retention and production of documents is included because of possible application of Section 1861(v)(1)(I) of the Social Security Act to this Agreement; if this Section should be found to be inapplicable, then this paragraph shall be deemed inoperative and without force and effect.

**k) Subcontracting or Assignment of Contract or Contract Funds**

Once awarded, this Contract shall not be subcontracted or assigned, in whole or in part, without the advance written approval of the Chief Procurement Officer, which approval shall be granted or withheld at the sole discretion of the Chief Procurement Officer. In no case, however, shall such approval relieve the Consultant from its obligations or change the terms of the Contract. The Consultant shall not transfer or assign any Contract funds or any interest therein due or to become due without the advance written approval of the Chief Procurement Officer. The unauthorized subcontracting or assignment of the Contract, in whole or in part, or the unauthorized transfer or assignment of any Contract funds, either in whole or in part, or any interest therein, which shall be due or are to become due the Consultant shall have no effect on the County and are null and void.

Prior to the commencement of the Contract, the Consultant shall identify in writing to the Chief Procurement Officer the names of any and all Subcontractors it intends to use in the performance of the Contract by completing the Identification of Subcontractor/Supplier/Subconsultant Form ("ISF"). The Chief Procurement Officer shall have the right to disapprove any Subcontractor. All Subcontractors shall be subject to the terms of this Contract. Consultant shall incorporate into all subcontracts all of the provisions of the Contract which affect such subcontract. Copies of subcontracts shall be provided to the Chief Procurement Officer upon request.

The Consultant must disclose the name and business address of each Subcontractor, attorney, lobbyist, accountant, consultant and any other person or entity whom the Consultant has retained or expects to retain in connection with the Matter, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant's regular payroll. "Lobbyist" means any person or entity who undertakes to influence any legislation or administrative action on behalf of any person or entity other than: (1) a not-for-profit entity, on an unpaid basis, or (2), himself.

"Lobbyist" also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action. If the Consultant is uncertain whether a disclosure is required under this Section, the Consultant must either ask the County, whether disclosure is required or make the disclosure.

The County reserves the right to prohibit any person from entering any County facility for any reason. All Consultants and Subcontractor of the Consultant shall be accountable to the Chief Procurement Officer or his designee while on any County property and shall abide by all rules and regulations imposed by the County.

**I) Professional Social Services**

In accordance with 34-146, of the Cook County Procurement Code, all Consultants or providers providing services under a Professional Social Service Contracts or Professional Social Services Agreements, shall submit an annual performance report to the Using Agency, i.e., the agency for whom the Consultant or provider is providing the professional social services, that includes but is not limited to relevant statistics, an empirical analysis where applicable, and a written narrative describing the goals and objectives of the contract or agreement and programmatic outcomes. The annual performance report shall be provided and reported to the Cook County Board of Commissioners by the applicable Using Agency within forty-five days of receipt. Failure of the Consultant or provider to provide an annual performance report will be considered a breach of contract or agreement by the Consultant or provider, and may result in termination of the Contract or agreement.

For purposes of this Section, a Professional Social Service Contract or Professional Social Service Agreement shall mean any contract or agreement with a social service provider, including other governmental agencies, nonprofit organizations, or for profit business enterprises engaged in the field of and providing social services, juvenile justice, mental health treatment, alternative sentencing, offender rehabilitation, recidivism reduction, foster care, substance abuse treatment, domestic violence services, community transitioning services, intervention, or such other similar services which provide mental, social or physical treatment and services to individuals. Said Professional Social Service Contracts or Professional Social Service Agreements do not include CCHHS managed care contracts that CCHHS may enter into with health care providers.

**ARTICLE 4) TERM OF PERFORMANCE**

**a) Term of Performance**

This Agreement takes effect when approved by the Cook County Board and its term shall begin on **January 28, 2019** ("Effective Date") and continue until **January 27, 2022** or until this Agreement is terminated in accordance with its terms, whichever occurs first.

**b) Timeliness of Performance**

- i) Consultant must provide the Services and Deliverables within the term and within the time limits required under this Agreement, pursuant to the provisions of Section 4.a and Exhibit 1. Further, Consultant acknowledges that TIME IS OF THE ESSENCE and that the failure of Consultant to comply with the time limits described in this Section 4.b may result in economic or other losses to the County.
- ii) Neither Consultant nor Consultant's agents, employees nor Subcontractors are entitled to any damages from the County, nor is any party entitled to be reimbursed by the County, for damages, charges or other losses or expenses incurred by Consultant by reason of delays or hindrances in the performance of the Services, whether or not caused by the County.

**c) Agreement Extension Option**

The Chief Procurement Officer may at any time before this Agreement expires elect to renew this Agreement for up to two (2) additional one-year periods under the same terms and conditions as this original Agreement, except as provided otherwise in this Agreement, by notice in writing to Consultant. After notification by the Chief Procurement Officer, this Agreement must be modified to reflect the time extension in accordance with the provisions of Section 10.c.

**ARTICLE 5) COMPENSATION**

**a) Basis of Payment**

The County will pay Consultant according to the Schedule of Compensation in the attached Exhibit 2 for the successful completion of services.

**b) Method of Payment**

All invoices submitted by the Consultant shall be in accordance with the cost provisions contained in the Agreement and shall contain a detailed description of the Deliverables, including the quantity of the Deliverables, for which payment is requested. All invoices for services shall include itemized entries indicating the date or time period in which the services were provided, the amount of time spent performing the services, and a detailed description of the services provided during the period of the invoice. All invoices shall reflect the amounts invoiced by and the amounts paid to the Consultant as of the date of the invoice. Invoices for new charges shall not include "past due" amounts, if any, which amounts must be set forth on a separate invoice. Consultant shall not be entitled to invoice the County for any late fees or other penalties.

In accordance with Section 34-177 of the Cook County Procurement Code, the County shall have a right to set off and subtract from any invoice(s) or Contract price, a sum equal to any fines and penalties, including interest, for any tax or fee delinquency and any debt or obligation owed by the Consultant to the County.

The Consultant acknowledges its duty to ensure the accuracy of all invoices submitted to the County for payment. By submitting the invoices, the Consultant certifies that all itemized entries set forth in the invoices are true and correct. The Consultant acknowledges that by submitting the invoices, it certifies that it has delivered the Deliverables, i.e., the goods, supplies, services or equipment set forth in the Agreement to the Using Agency, or that it has properly performed the services set forth in the Agreement. The invoice must also reflect the dates and amount of time expended in the provision of services under the Agreement. The Consultant acknowledges that any inaccurate statements or negligent or intentional misrepresentations in the invoices shall result in the County exercising all remedies available to it in law and equity including, but not limited to, a delay in payment or non-payment to the Consultant, and reporting the matter to the Cook County Office of the Independent Inspector General.

When a Consultant receives any payment from the County for any supplies, equipment, goods, or services, it has provided to the County pursuant to its Agreement, the Consultant must make payment to its Subcontractors within 15 days after receipt of payment from the County, provided that such Subcontractor has satisfactorily provided the supplies, equipment, goods or services in accordance with the Contract and provided the Consultant with all of the documents and information required of the Consultant. The Consultant may delay or postpone payment to a Subcontractor when the Subcontractor's supplies, equipment, goods, or services do not comply with the requirements of the Contract, the Consultant is acting in good faith, and not in retaliation for a Subcontractor exercising legal or contractual rights.

**c) Funding**

The source of funds for payments under this Agreement is identified in Exhibit 2, Schedule of Compensation. Payments under this Agreement must not exceed the dollar amount shown in Exhibit 2 without a written amendment in accordance with Section 10.c.

**d) Non-Appropriation**

If no funds or insufficient funds are appropriated and budgeted in any fiscal period of the County for payments to be made under this Agreement, then the County will notify Consultant in writing of that occurrence, and this Agreement will terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted. Payments for Services completed to the date of notification will be made to Consultant. No payments will be made or due to Consultant and under this Agreement beyond those amounts appropriated and budgeted by the County to fund payments under this Agreement.

e) **Taxes**

Federal Excise Tax does not apply to materials purchased by the County by virtue of Exemption Certificate No. 36-75-0038K. Illinois Retailers' Occupation Tax, Use Tax and Municipal Retailers' Occupation Tax do not apply to deliverables, materials or services purchased by the County by virtue of statute. The price or prices quoted herein shall include any and all other federal and/or state, direct and/or indirect taxes which apply to this Contract. The County's State of Illinois Sales Tax Exemption Identification No. is E-9998-2013-07.

f) **Price Reduction**

If at any time after the contract award, Consultant makes a general price reduction in the price of any of the Deliverables, the equivalent price reduction based on similar quantities and/or considerations shall apply to this Contract for the duration of the Contract period. For purposes of this Section 5.f., Price Reduction, a general price reduction shall include reductions in the effective price charged by Consultant by reason of rebates, financial incentives, discounts, value points or other benefits with respect to the purchase of the Deliverables. Such price reductions shall be effective at the same time and in the same manner as the reduction Consultant makes in the price of the Deliverables to its prospective customers generally.

g) **Consultant Credits**

To the extent the Consultant gives credits toward future purchases of goods or services, financial incentives, discounts, value points or other benefits based on the purchase of the materials or services provided for under this Contract, such credits belong to the County and not any specific Using Agency. Consultant shall reflect any such credits on its invoices and in the amounts it invoices the County.

## **ARTICLE 6) DISPUTES**

Any dispute arising under the Contract between the County and Consultant shall be decided by the Chief Procurement Officer. The complaining party shall submit a written statement detailing the dispute and specifying the specific relevant Contract provision(s) to the Chief Procurement Officer. Upon request of the Chief Procurement Officer, the party complained against shall respond to the complaint in writing within five days of such request. The Chief Procurement Officer will reduce her decision to writing and mail or otherwise furnish a copy thereof to the Consultant. The decision of the Chief Procurement Officer will be final and binding. Dispute resolution as provided herein shall be a condition precedent to any other action at law or in equity. However, unless a notice is issued by the Chief Procurement Officer indicating that additional time is required to review a dispute, the parties may exercise their contractual remedies, if any, if no decision is made within sixty (60) days following notification to the Chief Procurement Officer of a dispute. No inference shall be drawn from the absence of a decision by the Chief Procurement Officer.

Notwithstanding a dispute, Consultant shall continue to discharge all its obligations, duties and responsibilities set forth in the Contract during any dispute resolution proceeding unless otherwise agreed to by the County in writing.

## **ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS**

The Consultant, Subcontractor, licensees, grantees or persons or businesses who have a County contract, grant, license, or certification of eligibility for County contracts shall abide by all of the applicable provisions of the Office of the Independent Inspector General Ordinance (Section 2-281 et. seq. of the Cook County Code of Ordinances). Failure to cooperate as required may result in monetary and/or other penalties.

The Consultant shall observe and comply with the laws, ordinances, regulations and codes of the Federal, State, County and other local government agencies which may in any manner affect the performance of the Contract including, but not limited to, those County Ordinances set forth in the Certifications attached hereto and incorporated herein. Assurance of compliance with this requirement by the Consultant's employees, agents or Subcontractor shall be the responsibility of the Consultant.

The Consultant shall secure and pay for all federal, state and local licenses, permits and fees required hereunder.

## **ARTICLE 8) SPECIAL CONDITIONS**

### **a) Warranties and Representations**

In connection with signing and carrying out this Agreement, Consultant:

- i) warrants that Consultant is appropriately licensed under Illinois law to perform the Services required under this Agreement and will perform no Services for which a professional license is required by law and for which Consultant is not appropriately licensed;
- ii) warrants it is financially solvent; it and each of its employees, agents and Subcontractors of any tier are competent to perform the Services required under this Agreement; and Consultant is legally authorized to execute and perform or cause to be performed this Agreement under the terms and conditions stated in this Agreement;
- iii) warrants that it will not knowingly use the services of any ineligible consultant or Subcontractor for any purpose in the performance of its Services under this Agreement;

- iv) warrants that Consultant and its Subcontractors are not in default at the time this Agreement is signed, and has not been considered by the Chief Procurement Officer to have, within 5 years immediately preceding the date of this Agreement, been found to be in default on any contract awarded by the County;
- v) represents that it has carefully examined and analyzed the provisions and requirements of this Agreement; it understands the nature of the Services required; from its own analysis it has satisfied itself as to the nature of all things needed for the performance of this Agreement; this Agreement is feasible of performance in accordance with all of its provisions and requirements, and Consultant warrants it can and will perform, or cause to be performed, the Services in strict accordance with the provisions and requirements of this Agreement;
- vi) represents that Consultant and, to the best of its knowledge, its Subcontractors are not in violation of the provisions of the Illinois Criminal Code, 720 ILCS 5/33E as amended; and
- vii) acknowledges that any certification, affidavit or acknowledgment made under oath in connection with this Agreement is made under penalty of perjury and, if false, is also cause for termination under Sections 9.a and 9.c.

**b) Ethics**

- i) In addition to the foregoing warranties and representations, Consultant warrants:
  - (1) no officer, agent or employee of the County is employed by Consultant or has a financial interest directly or indirectly in this Agreement or the compensation to be paid under this Agreement except as may be permitted in writing by the Board of Ethics.
  - (2) no payment, gratuity or offer of employment will be made in connection with this Agreement by or on behalf of any Subcontractors to the prime Consultant or higher tier Subcontractors or anyone associated with them, as an inducement for the award of a subcontract or order.

**c) Joint and Several Liability**

If Consultant, or its successors or assigns, if any, is comprised of more than one individual or other legal entity (or a combination of them), then under this Agreement, each and without limitation every obligation or undertaking in this Agreement to be fulfilled or performed by Consultant is the joint and several obligation or undertaking of each such individual or other legal entity.

d) **Business Documents**

At the request of the County, Consultant must provide copies of its latest articles of incorporation, by-laws and resolutions, or partnership or joint venture agreement, as applicable.

e) **Conflicts of Interest**

- i) No member of the governing body of the County or other unit of government and no other officer, employee or agent of the County or other unit of government who exercises any functions or responsibilities in connection with the Services to which this Agreement pertains is permitted to have any personal interest, direct or indirect, in this Agreement. No member of or delegate to the Congress of the United States or the Illinois General Assembly and no Commissioner of the Cook County Board or County employee is allowed to be admitted to any share or part of this Agreement or to any financial benefit to arise from it.
- ii) Consultant covenants that it, and to the best of its knowledge, its Subcontractors if any (collectively, "**Consulting Parties**"), presently have no direct or indirect interest and will not acquire any interest, direct or indirect, in any project or contract that would conflict in any manner or degree with the performance of its Services under this Agreement.
- iii) Upon the request of the County, Consultant must disclose to the County its past client list and the names of any clients with whom it has an ongoing relationship. Consultant is not permitted to perform any Services for the County on applications or other documents submitted to the County by any of Consultant's past or present clients. If Consultant becomes aware of a conflict, it must immediately stop work on the assignment causing the conflict and notify the County.
- iv) Without limiting the foregoing, if the Consulting Parties assist the County in determining the advisability or feasibility of a project or in recommending, researching, preparing, drafting or issuing a request for proposals or bid specifications for a project, the Consulting Parties must not participate, directly or indirectly, as a prime, Subcontractor or joint venturer in that project or in the preparation of a proposal or bid for that project during the term of this Agreement or afterwards. The Consulting Parties may, however, assist the County in reviewing the proposals or bids for the project if none of the Consulting Parties have a relationship with the persons or entities that submitted the proposals or bids for that project.

- v) The Consultant further covenants that, in the performance of this Agreement, no person having any conflicting interest will be assigned to perform any Services or have access to any confidential information, as defined in Section 3.h of this Agreement. If the County, by the Chief Procurement Officer in his reasonable judgment, determines that any of Consultant's Services for others conflict with the Services Consultant is to render for the County under this Agreement, Consultant must terminate such other services immediately upon request of the County.
- vi) Furthermore, if any federal funds are to be used to compensate or reimburse Consultant under this Agreement, Consultant represents that it is and will remain in compliance with federal restrictions on lobbying set forth in Section 319 of the Department of the Interior and Related Agencies Appropriations Act for Fiscal year 1990, 31 U.S.C. § 1352, and related rules and regulations set forth at 54 Fed. Reg. 52,309 ff. (1989), as amended. If federal funds are to be used, Consultant must execute a Certification Regarding Lobbying, which will be attached as an exhibit and incorporated by reference as if fully set forth here.

**f) Non-Liability of Public Officials**

Consultant and any assignee or Subcontractor of Consultant must not charge any official, employee or agent of the County personally with any liability or expenses of defense or hold any official, employee or agent of the County personally liable to them under any term or provision of this Agreement or because of the County's execution, attempted execution or any breach of this Agreement.

**ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET**

**a) Events of Default Defined**

The following constitute events of default:

- i) Any material misrepresentation, whether negligent or willful and whether in the inducement or in the performance, made by Consultant to the County.
- ii) Consultant's material failure to perform any of its obligations under this Agreement including the following:
  - (a) Failure due to a reason or circumstances within Consultant's reasonable control to perform the Services with sufficient personnel and equipment or with sufficient material to ensure the performance of the Services;

- (b) Failure to perform the Services in a manner reasonably satisfactory to the Chief Procurement Officer or inability to perform the Services satisfactorily as a result of insolvency, filing for bankruptcy or assignment for the benefit of creditors;
  - (c) Failure to promptly re-perform within a reasonable time Services that were rejected as erroneous or unsatisfactory;
  - (d) Discontinuance of the Services for reasons within Consultant's reasonable control; and
  - (e) Failure to comply with any other material term of this Agreement, including the provisions concerning insurance and nondiscrimination.
- iii) Any change in ownership or control of Consultant without the prior written approval of the Chief Procurement Officer, which approval the Chief Procurement Officer will not unreasonably withhold.
  - iv) Consultant's default under any other agreement it may presently have or may enter into with the County during the life of this Agreement. Consultant acknowledges and agrees that in the event of a default under this Agreement the County may also declare a default under any such other Agreements.
  - v) Failure to comply with Article 7 in the performance of the Agreement.
  - vi) Consultant's repeated or continued violations of County ordinances unrelated to performance under the Agreement that in the opinion of the Chief Procurement Officer indicate a willful or reckless disregard for County laws and regulations.

**b) Remedies**

The occurrence of any event of default permits the County, at the County's sole option, to declare Consultant in default. The Chief Procurement Officer may in his sole discretion give Consultant an opportunity to cure the default within a certain period of time, which period of time must not exceed 30 days, unless extended by the Chief Procurement Officer. Whether to declare Consultant in default is within the sole discretion of the Chief Procurement Officer and neither that decision nor the factual basis for it is subject to review or challenge under the Disputes provision of this Agreement.

The Chief Procurement Officer will give Consultant written notice of the default, either in the form of a cure notice ("Cure Notice"), or, if no opportunity to cure will be granted, a default notice ("Default Notice"). If the Chief Procurement Officer gives a Default Notice, he will also indicate any present intent he may have to terminate this Agreement, and the decision to terminate (but not the decision not to terminate) is final and effective upon giving the notice. The Chief Procurement Officer may give a Default Notice if Consultant fails to affect a cure within the cure period given in a Cure Notice. When a Default Notice with intent to terminate is given as provided in this Section 9.b and Article 11, Consultant must discontinue any Services, unless otherwise directed in the notice, and deliver all materials accumulated in the performance of this Agreement, whether completed or in the process, to the County. After giving a Default Notice, the County may invoke any or all of the following remedies:

- i) The right to take over and complete the Services, or any part of them, at Consultant's expense and as agent for Consultant, either directly or through others, and bill Consultant for the cost of the Services, and Consultant must pay the difference between the total amount of this bill and the amount the County would have paid Consultant under the terms and conditions of this Agreement for the Services that were assumed by the County as agent for the Consultant under this Section 9.b;
- ii) The right to terminate this Agreement as to any or all of the Services yet to be performed effective at a time specified by the County;
- iii) The right of specific performance, an injunction or any other appropriate equitable remedy;
- iv) The right to money damages;
- v) The right to withhold all or any part of Consultant's compensation under this Agreement;
- vi) The right to consider Consultant non-responsible in future contracts to be awarded by the County.

If the Chief Procurement Officer considers it to be in the County's best interests, he may elect not to declare default or to terminate this Agreement. The parties acknowledge that this provision is solely for the benefit of the County and that if the County permits Consultant to continue to provide the Services despite one or more events of default, Consultant is in no way relieved of any of its responsibilities, duties or obligations under this Agreement, nor does the County waive or relinquish any of its rights.

The remedies under the terms of this Agreement are not intended to be exclusive of any other remedies provided, but each and every such remedy is cumulative and is in addition to any other remedies, existing now or later, at law, in equity or by statute. No delay or omission to exercise any right or power accruing upon any event of default impairs any

such right or power, nor is it a waiver of any event of default nor acquiescence in it, and every such right and power may be exercised from time to time and as often as the County considers expedient.

**c) Early Termination**

In addition to termination under Sections 9.a and 9.b of this Agreement, the County may terminate this Agreement, or all or any portion of the Services to be performed under it, at any time by a notice in writing from the County to Consultant. The County will give notice to Consultant in accordance with the provisions of Article 11. The effective date of termination will be the date the notice is received by Consultant or the date stated in the notice, whichever is later. If the County elects to terminate this Agreement in full, all Services to be provided under it must cease and all materials that may have been accumulated in performing this Agreement, whether completed or in the process, must be delivered to the County effective 10 days after the date the notice is considered received as provided under Article 11 of this Agreement (if no date is given) or upon the effective date stated in the notice.

After the notice is received, Consultant must restrict its activities, and those of its Subcontractors, to winding down any reports, analyses, or other activities previously begun. No costs incurred after the effective date of the termination are allowed. Payment for any Services actually and satisfactorily performed before the effective date of the termination is on the same basis as set forth in Article 5, but if any compensation is described or provided for on the basis of a period longer than 10 days, then the compensation must be prorated accordingly. No amount of compensation, however, is permitted for anticipated profits on unperformed Services. The County and Consultant must attempt to agree on the amount of compensation to be paid to Consultant, but if not agreed on, the dispute must be settled in accordance with Article 6 of this Agreement. The payment so made to Consultant is in full settlement for all Services satisfactorily performed under this Agreement.

Consultant must include in its contracts with Subcontractors an early termination provision in form and substance equivalent to this early termination provision to prevent claims against the County arising from termination of subcontracts after the early termination. Consultant will not be entitled to make any early termination claims against the County resulting from any Subcontractor's claims against Consultant or the County to the extent inconsistent with this provision.

If the County's election to terminate this Agreement for default under Sections 9.a and 9.b is determined in a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered to be an early termination under this Section 9.c.

**d) Suspension**

The County may at any time request that Consultant suspend its Services, or any part of them, by giving 15 days prior written notice to Consultant or upon informal oral, or even

no notice, in the event of emergency. No costs incurred after the effective date of such suspension are allowed. Consultant must promptly resume its performance of the Services under the same terms and conditions as stated in this Agreement upon written notice by the Chief Procurement Officer and such equitable extension of time as may be mutually agreed upon by the Chief Procurement Officer and Consultant when necessary for continuation or completion of Services. Any additional costs or expenses actually incurred by Consultant as a result of recommencing the Services must be treated in accordance with the compensation provisions under Article 5 of this Agreement.

No suspension of this Agreement is permitted in the aggregate to exceed a period of 45 days within any one year of this Agreement. If the total number of days of suspension exceeds 45 days, Consultant by written notice may treat the suspension as an early termination of this Agreement under Section 9.c.

**e) Right to Offset**

In connection with performance under this Agreement, the County may offset any excess costs incurred:

- i) if the County terminates this Agreement for default or any other reason resulting from Consultant's performance or non-performance;
- ii) if the County exercises any of its remedies under Section 9.b of this Agreement; or
- iii) if the County has any credits due or has made any overpayments under this Agreement.

The County may offset these excess costs by use of any payment due for Services completed before the County terminated this Agreement or before the County exercised any remedies. If the amount offset is insufficient to cover those excess costs, Consultant is liable for and must promptly remit to the County the balance upon written demand for it. This right to offset is in addition to and not a limitation of any other remedies available to the County.

**f) Delays**

Consultant agrees that no charges or claims for damages shall be made by Consultant for any delays or hindrances from any cause whatsoever during the progress of any portion of this Contract.

**g) Prepaid Fees**

In the event this Contract is terminated by either party, for cause or otherwise, and the County has prepaid for any Deliverables, Consultant shall refund to the County, on a prorated basis to the effective date of termination, all amounts prepaid for Deliverables not actually

provided as of the effective date of the termination. The refund shall be made within fourteen (14) days of the effective date of termination.

## **ARTICLE 10) GENERAL CONDITIONS**

### **a) Entire Agreement**

#### **i) General**

This Agreement, and the exhibits attached to it and incorporated in it, constitute the entire agreement between the parties and no other warranties, inducements, considerations, promises or interpretations are implied or impressed upon this Agreement that are not expressly addressed in this Agreement.

#### **ii) No Collateral Agreements**

Consultant acknowledges that, except only for those representations, statements or promises expressly contained in this Agreement and any exhibits attached to it and incorporated by reference in it, no representation, statement or promise, oral or in writing, of any kind whatsoever, by the County, its officials, agents or employees, has induced Consultant to enter into this Agreement or has been relied upon by Consultant, including any with reference to:

- (a) the meaning, correctness, suitability or completeness of any provisions or requirements of this Agreement;
- (b) the nature of the Services to be performed;
- (c) the nature, quantity, quality or volume of any materials, equipment, labor and other facilities needed for the performance of this Agreement;
- (d) the general conditions which may in any way affect this Agreement or its performance;
- (e) the compensation provisions of this Agreement; or
- (f) any other matters, whether similar to or different from those referred to in (a) through (e) immediately above, affecting or having any connection with this Agreement, its negotiation, any discussions of its performance or those employed or connected or concerned with it.

#### **iii) No Omissions**

Consultant acknowledges that Consultant was given an opportunity to review all documents forming this Agreement before signing this Agreement in order that it might request inclusion in this Agreement of any statement, representation, promise or provision that it desired or on that it wished to place reliance. Consultant did so

review those documents, and either every such statement, representation, promise or provision has been included in this Agreement or else, if omitted, Consultant relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Agreement in its entirety without claiming reliance on it or making any other claim on account of its omission.

**b) Counterparts**

This Agreement is comprised of several identical counterparts, each to be fully signed by the parties and each to be considered an original having identical legal effect.

**c) Contract Amendments**

The parties may during the term of the Contract make amendments to the Contract but only as provided in this section. Such amendments shall only be made by mutual agreement in writing.

In the case of Contracts not approved by the Board, the Chief Procurement Officer may amend a contract provided that any such amendment does not extend the Contract by more than one (1) year, and further provided that the total cost of all such amendments does not increase the total amount of the Contract beyond \$150,000. Such action may only be made with the advance written approval of the Chief Procurement Officer. If the amendment extends the Contract beyond one (1) year or increases the total award amount beyond \$150,000, then Board approval will be required.

No Using Agency or employee thereof has authority to make any amendments to this Contract. Any amendments to this Contract made without the express written approval of the Chief Procurement Officer is void and unenforceable.

Consultant is hereby notified that, except for amendments which are made in accordance with this Section 10.c. Contract Amendments, no Using Agency or employee thereof has authority to make any amendment to this Contract.

**d) Governing Law and Jurisdiction**

This Contract shall be governed by and construed under the laws of the State of Illinois. The Consultant irrevocably agrees that, subject to the County's sole and absolute election to the contrary, any action or proceeding in any way, manner or respect arising out of the Contract, or arising from any dispute or controversy arising in connection with or related to the Contract, shall be litigated only in courts within the Circuit Court of Cook County, State of Illinois, and the Consultant consents and submits to the jurisdiction thereof. In accordance with these provisions, Consultant waives any right it may have to transfer or change the venue of any litigation brought against it by the County pursuant to this Contract.

**e) Severability**

If any provision of this Agreement is held or considered to be or is in fact invalid, illegal, inoperative or unenforceable as applied in any particular case in any jurisdiction or in all cases because it conflicts with any other provision or provisions of this Agreement or of any constitution, statute, ordinance, rule of law or public policy, or for any other reason, those circumstances do not have the effect of rendering the provision in question invalid, illegal, inoperative or unenforceable in any other case or circumstances, or of rendering any other provision or provisions in this Agreement invalid, illegal, inoperative or unenforceable to any extent whatsoever. The invalidity, illegality, inoperativeness or unenforceability of any one or more phrases, sentences, clauses or sections in this Agreement does not affect the remaining portions of this Agreement or any part of it.

**f) Assigns**

All of the terms and conditions of this Agreement are binding upon and inure to the benefit of the parties and their respective legal representatives, successors and assigns.

**g) Cooperation**

Consultant must at all times cooperate fully with the County and act in the County's best interests. If this Agreement is terminated for any reason, or if it is to expire on its own terms, Consultant must make every effort to assure an orderly transition to another provider of the Services, if any, orderly demobilization of its own operations in connection with the Services, uninterrupted provision of Services during any transition period and must otherwise comply with the reasonable requests and requirements of the Using Agency in connection with the termination or expiration.

**h) Waiver**

Nothing in this Agreement authorizes the waiver of a requirement or condition contrary to law or ordinance or that would result in or promote the violation of any federal, state or local law or ordinance.

Whenever under this Agreement the County by a proper authority waives Consultant's performance in any respect or waives a requirement or condition to either the County's or Consultant's performance, the waiver so granted, whether express or implied, only applies to the particular instance and is not a waiver forever or for subsequent instances of the performance, requirement or condition. No such waiver is a modification of this Agreement regardless of the number of times the County may have waived the performance, requirement or condition. Such waivers must be provided to Consultant in writing.

i) **Independent Consultant**

This Agreement is not intended to and will not constitute, create, give rise to, or otherwise recognize a joint venture, partnership, corporation or other formal business association or organization of any kind between Consultant and the County. The rights and the obligations of the parties are only those expressly set forth in this Agreement. Consultant must perform under this Agreement as an independent Consultant and not as a representative, employee, agent, or partner of the County.

This Agreement is between the County and an independent Consultant and, if Consultant is an individual, nothing provided for under this Agreement constitutes or implies an employer-employee relationship such that:

- i) The County will not be liable under or by reason of this Agreement for the payment of any compensation award or damages in connection with the Consultant performing the Services required under this Agreement.
- ii) Consultant is not entitled to membership in the County Pension Fund, Group Medical Insurance Program, Group Dental Program, Group Vision Care, Group Life Insurance Program, Deferred Income Program, vacation, sick leave, extended sick leave, or any other benefits ordinarily provided to individuals employed and paid through the regular payrolls of the County.
- iv) The County is not required to deduct or withhold any taxes, FICA or other deductions from any compensation provided to the Consultant.

j) **Governmental Joint Purchasing Agreement**

Pursuant to Section 4 of the Illinois Governmental Joint Purchasing Act (30 ILCS 525) and the Joint Purchase Agreement approved by the Cook County Board of Commissioners (April 9, 1965), other units of government may purchase goods or services under this contract.

In the event that other agencies participate in a joint procurement, the County reserves the right to renegotiate the price to accommodate the larger volume.

k) **Comparable Government Procurement**

As permitted by the County of Cook, other government entities, if authorized by law, may wish to purchase the goods, supplies, services or equipment under the same terms and conditions contained in this Contract (i.e., comparable government procurement). Each entity wishing to reference this Contract must have prior authorization from the County of Cook and the Consultant. If such participation is authorized, all purchase orders will be issued directly from and shipped directly to the entity requiring the goods, supplies, equipment or services supplies/services. The County shall not be held responsible for any orders placed, deliveries made or payment for the goods, supplies, equipment or services

supplies/services ordered by these entities. Each entity reserves the right to determine the amount of goods, supplies, equipment or services it wishes to purchase under this Contract.

I) **Force Majeure**

Neither Consultant nor County shall be liable for failing to fulfill any obligation under this Contract if such failure is caused by an event beyond such party's reasonable control and which is not caused by such party's fault or negligence. Such events shall be limited to acts of God, acts of war, fires, lightning, floods, epidemics, or riots.

**ARTICLE 11) NOTICES**

All notices required pursuant to this Contract shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if hand delivered or if deposited in the United States mail, postage prepaid, registered or certified, return receipt requested. Notice as provided herein does not waive service of summons or process.

If to the County:      Cook County Adult Probation  
69 W. Washington Street, Suite 1940  
Chicago, Illinois 60602  
Attention: Department Director

Cook County Juvenile Probation and Court Services Department  
1100 South Hamlin Avenue  
Chicago, Illinois 60612  
Attention: Department Director

Cook County Sheriff  
50 W. Washington Street  
Chicago, Illinois 60602  
Attention: Department Director

and

Cook County Chief Procurement Officer  
118 North Clark Street, Room 1018  
Chicago, Illinois 60602  
(Include County Contract Number on all notices)

If to Consultant:      Track Group, Inc.  
200 E. 5<sup>th</sup> Avenue, Unit 100  
Naperville, IL 60563  
Attention: Matthew Swando

Changes in these addresses must be in writing and delivered in accordance with the provisions of this Article 11. Notices delivered by mail are considered received three days after mailing in accordance with this Article 11. Notices delivered personally are considered effective upon receipt. Refusal to accept delivery has the same effect as receipt.

## **ARTICLE 12) AUTHORITY**

Execution of this Agreement by Consultant is authorized by a resolution of its Board of Directors, if a corporation, or similar governing document, and the signature(s) of each person signing on behalf of Consultant have been made with complete and full authority to commit Consultant to all terms and conditions of this Agreement, including each and every representation, certification and warranty contained in it, including the representations, certifications and warranties collectively incorporated by reference in it.

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 1

Scope of Services

# Statement of Work

## 1. INTRODUCTION

This Statement of Work ("SOW") is intended to document the scope, roles, responsibilities, terms and conditions, tasks and timeframe for Global Positioning System (GPS) equipment and services for an electronic monitoring system designed to monitor individuals' compliance with home detention and curfew orders and to monitor stay away orders for those charged with/or convicted of domestic violence related offenses at Cook County, Illinois (the "County"). Breaches will result in immediate notification to law enforcement, the victim and the supervising agency. Track Group (hereinafter referred to as "Vendor" or "Track Group") will provide an GPS electronic monitoring program for the Cook County Sheriff's Office ("Sheriff's Office"), the Juvenile Probation Department ("Juvenile Probation"), and the Circuit Court of Cook County Adult Probation Department ("Adult Probation").

The Sheriff's Office, Juvenile Probation, and Adult Probation are distinct entities with distinct electronic monitoring programs, as described herein. Accordingly, Vendor shall tailor unique alert notification protocols, billing, and statistical reports for each program. The scope of services for all departments includes, but is not limited to the following:

1. Providing complete electronic monitoring services that includes receiving and processing all alerts.
2. Providing maintenance and consumables for leased Cook County equipment.
3. Maintaining all data from Cook County equipment at the Proposer's facility.
4. Developing and interfacing a dispatching and permissions process with Cook County.
5. Creating and maintaining a web-based case management application.

### 1.1 Using Agency - Cook County Sheriff's Office

The Sheriff's Office operates the Cook County Jail, one of the largest single-site county facilities in the United States. Primarily holding pre-trial detainees, CCSO processes approximately 100,000 detainees annually and averages a daily population within Cook County Jail of approximately 7,600, with a custodial population averaging 9,600 daily that includes electronic monitoring.

The Sheriff's Office has maintained an electronic monitoring program since 1989, currently populated by individuals court-ordered to its programs as a condition of pre-trial bond, as a sentence, or as part of post-release reintegration. Currently, the Sheriff's Office utilizes RF units that are approximately ninety-nine percent (99%) cellular units. The Sheriff's Office reserves the right under this contract to "activate," expand, and/or limit use of GPS monitoring services at its sole discretion and in accordance with the terms contained herein.

### 1.2 Using Agency – Juvenile Probation

The Juvenile Probation and Court Services Department Circuit Court of Cook County implemented an Electronic Monitoring Program in June of 1996. The Electronic Monitoring Program initially utilized

landline units and over time, the department transitioned to cellular technology. In January 2010, the Cook County Juvenile Probation and Court Services Department upgraded the electronic monitoring technology transitioning 100 % of the devices to global positioning satellite (GPS) devices.

Minors in pre-adjudication stage of proceedings with a finding of probable cause and urgent and immediate necessity and minors in post adjudication stage in jeopardy of secure detention may be placed in their homes under an order of home confinement with electronic monitoring. Minors qualifying for this alternative include youth found to be in urgent and immediate necessity of secure detention due to a new offense, violations of probation, or as a consequence for being apprehended on a Juvenile Arrest Warrant. The program is limited to 45 days in lieu of secure detention.

The Juvenile Probation and Court Services Department services up to 300 clients at any given time.

### **1.3 Using Agency - Adult Probation**

Operating under the Office of the Chief Judge, the Adult Probation Department administers a wide range of programs covering both standard and specialized probation supervision and pretrial and presentence services. The majority of Adult Probation's resources are dedicated to supervising criminal offenders sentenced to probation, which is a sentencing option that requires individuals to comply with specific conditions while residing in the community. Probation officers assist individuals in complying with their sentences through guidance, surveillance, and referrals to service providers for treatment, education, and employment services. Officers notify the court when probationers/participants fail to comply with conditions of their sentence.

Each year Adult Probation receives over 12,500 new probation cases and has an average daily caseload of approximately 24,000 probationers/participants. About 86% of Adult Probation's caseload is composed of felons and 14% of misdemeanants. Eighty-seven percent of probationers/participants are assigned to standard caseload supervision, while 13% are supervised in specialized programs designed for specific offender populations. These programs include the Adult Sex Offender Program, the Mental Health Unit and Mental Health Courts, Intensive Probation Supervision, the Gang Intervention Unit, the Intensive Drug Program, Cook County's Drug Treatment and Veterans' Courts, and Domestic Violence Supervision. Through its Pretrial Services Division, Adult Probation supervises defendants released on bond and conducts pre-bail interviews to assist the courts in making decisions about bond/pretrial supervision.

Adult Probation's Home Confinement Unit monitors both pretrial defendants and probationers/participants ordered to GPS monitoring for domestic violence related offenses. Adult Probation currently has approximately 325 defendants/ probationers /participants being supervised through GPS technology and approximately 100 victims with a mobile device participating in the GPS program.

## **2. SERVICES**

This Section describes the services for this Agreement that shall apply to all Using Departments. Vendor is responsible for meeting all requirements, specifications, terms, and conditions listed in this section unless explicitly stated otherwise herein.

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 GPS

Track Group shall provide and maintain equipment necessary for the provision of the services described herein. All Track Group equipment provided under this Agreement shall be leased to the County for the Agreement term. Any Track Group equipment in County's possession, custody or control shall be used in accordance with the manufacturing specifications and recommendations. The scope of services provided by Track Group and its subcontractors for all departments includes, but is not limited to, the following: participant monitoring equipment; monitoring center services; field technicians to install, trouble shoot, and clean equipment; manage inventory; provide on-going maintenance; training services; and all reports required by the County with regards to the GPS Monitoring Program.

Track Group shall operate its participant monitoring center twenty-four (24) hours per day, seven (7) days per week, 365 days per year. Track Group shall provide the County with sufficient electronic monitoring equipment (plus a shelf inventory equivalent to 30% of the total number of units that are in use) and all consumables in order for each Using Department to operate its program, with consideration to the fact that participant populations fluctuate. Neither the County nor any Using Department makes any guarantee as to the number of individuals that may be monitored or the length of time each participant may be monitored. Track Group shall provide services regardless of the actual number of participants or length of time for each participant.

Each Using Department will notify Track Group of the need to perform equipment installations and removals. Once Track Group staff are notified through the agreed upon transmittals that an offender has completed the program or should be removed from the program, the offender will be deactivated from the system and a retrieval order will be initiated. Once the notification has been received to remove the client from the program, the equipment (inventory) assigned to that offender will be removed from the Agency inventory upon system deactivation and shall not count against the Agency's shelf allowance pending retrieval or drop-off. –Track Group shall be solely responsible for the cost of all lost, damaged, or stolen equipment and the replacements.

County will use the necessary paperwork and transmittals that are required to ensure Track Group has the appropriate information in order to properly monitor a participant. This includes, but is not limited to, providing complete participant information forms to the Track Group's office when requesting that a participant be enrolled on electronic monitoring. Both ADP staff and Track Group have the ability to enroll/schedule/active/monitor an offender or victim via the monitoring software platform. Track Group will complete any and all requested enrollments into the system within two (2) hours of receipt of a request for enrollment via the proper transmittals, and all pertinent client information.

County will provide Track Group with the permanent schedule to be in effect for the participant while monitored by Consultant.

Track Group will provide alert notifications to local law enforcement, the victim and the supervising agency according to agreed-upon departmental protocols established by each individual agency and via live operator voice communication and automated text messages/emails. Track Group will agree to provide any data or reports necessary to assist with the enforcement of violations.

Track Group shall not include County's name in listings of its customers, without the express written permission of County.

Track Group shall provide a web based system that has the ability to interface with Using Departments' case management system(s).

## 2.1 Active GPS General System Requirements

Track Group's GPS monitoring system shall comply with the following minimum requirements, in addition to the specifications set forth within this Statement of Work.

- A. 24/7/365 Participant Tracking System.** Track Group's GPS monitoring system includes the following equipment, software and services, as shown in the technical specifications documents included in Exhibit 1 to the Statement of Work

Equipment:

- *Shadow™ - One-piece GPS device*
- *ReliAlert™XC3 – One-piece GPS device with 2/3-way live voice communication*
- *Victim App – Smartphone application for victim*
- *When requested, Track Group will provide a smartphone preloaded with the Victim App at the rates set forth in the Schedule of Compensation*
- *ReliAlert™XC3 Standard Strap (in all sizes needed)*
- *SecureCuff™ (Optional) – Strap w/encased steel band for ReliAlert™XC3*
- *RF Beacon™ (Optional) – Utilized in conjunction with Shadow™ or ReliAlert™XC3*
- *Consumables – included per Schedule of Compensation*

Software:

- *TrackerPAL™ Operating Platform – Monitoring software platform*
- *TrackerPAL™ Mobile Application – Mobile application of TrackerPAL™*
- *Data Analytics (Optional) – Analytics application providing statistical analysis procedures, data and text mining, and predictive modeling*

Services:

- *Monitoring Center Services - Live 24/7/365 monitoring of all alarms, alert responses according to Agency protocols that include immediate text and/or email, live phone call notification to local law enforcement (as directed by Agency), the victim and supervising Agency staff, in addition to customer and technical support.*
- *Customer Support Services – Account management and customers support services team for account and technical support.*

- B. Real-Time Alerts & Immediate Notification.** Track Group's GPS system includes two (2) single-unit, GPS devices (ReliAlert™XC3 and Shadow™) that communicate directly with the TrackerPAL™ monitoring system via 3G cellular channels from available cellular networks. The device captures and transmits participant location and event information every minute to the TrackerPAL™ system – alarms are transmitted when they occur. Notification is made according to Agency

protocols that include immediate text and/or email, live phone call notification to local law enforcement (as directed by Agency), the victim, and supervising Agency staff.

- C. **GPS Units.** Track Group will initially provide the County with approximately 825 GPS devices for the expected transition of active GPS devices/participants; as well as the required 30% inventory allowance and all consumables. Track Group is fully capable of providing additional devices, should any or all Using Department's program growth require it.
- D. **Provision of Additional Units.** Track Group will provide each Department the required 30% shelf stock (based on active devices) and all consumables at no cost until activated on a participant. If additional units are requested by a Department, Track Group's local equipment fulfillment center enables delivery of units within 24 hours, including weekends and holidays. All shipping/delivery costs are the sole responsibility of Track Group.
- E. **Immediate Electronic Alert Notifications.** Shadow™ and ReliAlert™XC3 GPS devices, along with the TrackerPAL™ monitoring system, recognize violations and immediately generate automated alert notifications via text and email to designated County personnel and victims based upon pre-established notification protocols created by each agency. Live phone call notification to local law enforcement, the victim and the supervising agency can be made by the Monitoring Center upon violation notification within the monitoring system alarm queue – notification is also based upon pre-established notification protocols.
- F. **Communication with Participant.** ReliAlert™XC3 has on-board two/three-way live voice communication technology so that the Track Group Monitoring Center can contact the participant directly in response to violations and in accordance with protocols established by the supervising officer. Authorized County personnel can contact the Track Group Monitoring Center and request a call-bridge to the device to speak directly to the participant at any time. The Monitoring Center operator remains on the call to provide assistance (three-way call).

ReliAlert™XC3 also allows the participant to place a call (via a button on top of the device) directly to the Track Group Monitoring Center in cases of emergency. All calls to and from the ReliAlert™XC3 device are automatically digitally recorded, time stamped, and archived so that audio files can be provided on request.

- G. **Immediate GPS Alert Information Notification.** Alert notification protocols can be established by County authorized personnel, within the TrackerPAL™ software interface, by alarm type. Notification methods include text message, email and live phone call and are either automatically initiated by the TrackerPAL™ system or handled by the Track Group Monitoring Center upon receipt of an alert and with pre-established agency protocols. Victim notification is also included in the violation notification protocols and includes text message, email or live phone call by the Monitoring Center.
- H. **Central Host System Location and Responsibility.** TrackerPAL™ resides on an IBM secured and redundant system. The IBM System is SSAE 16, ISO 27001, SOC2 and Safe Harbor Compliant and the Infrastructure covers redundant networking, power and infrastructure. Systems are monitored by IBM Managed Services 24 hours, seven days a week; augmenting by Track Group's

IT team in ensuring that the physical environment is both stable and secure. The location is hardened against physical intrusion, and server room access is limited to certified employees. All controls (inside and outside the data center) are vetted by third-party auditors. Track Group is fully responsible for the TrackerPAL™ system.

- I. **GPS Equipment Accuracy within 50 Feet.** The GPS receivers in ReliAlert™XC3 and Shadow™ devices feature extremely low power requirements, increased sensitivity, accurate GPS acquisition capabilities and advanced jamming suppression mechanisms to ensure maximum GPS performance even in hostile environments and enables accuracy to within 50 feet in a normal operating environment. Each location point is depicted in the software as either a “high confidence” point (accurate to within approximately 30-40 feet), or a “medium confidence” point (accurate to within approximately 100-130-40 feet).
- J. **Supplemental or enhanced tracking system when GPS is unavailable or diminished.** Both Shadow™ and ReliAlert™XC3 include secondary locationing technology. Once a device recognizes a loss of the GPS signal, it automatically provides cellular triangulation as a secondary means of tracking.

## **2.2 Active Global Positioning Equipment**

Track Group’s products and services are flexible and can be customized as necessary for Cook County Sheriff’s Office, Adult Probation Department and Juvenile Probation Department. Track Group shall provide the most recent commercially utilized technology that meets all current industry standards of detention facilities and probation departments to effectively and efficiently monitor participants, at no additional cost to the County. Track Group shall obtain approval from each and all Using Department(s) prior to implementing any significant changes in the equipment and/or software utilized for monitoring participants.

### **2.2.1 Active GPS Alerts**

Track Group’s system will generate an immediate alert specifically identified by type (e.g., exclusion zone alert, inclusion zone alert, tamper alert, low-battery alert, no communication/no location alert, and etc.), with an alert timeframe that may be customizable by the County. Shadow™ and ReliAlert™XC3 devices, in conjunction with the TrackerPAL™ monitoring system, recognize and generate an immediate alert upon violation. These alerts are specifically identified by type and reflected in the TrackerPAL™ software; as well as in the alert notification sent to County personnel, the victim and local law enforcement, based upon agency-defined notification protocols.

### **2.2.2 Active GPS Device/Hardware Equipment**

- A. **Verbal communication with participants 24/7/365.** ReliAlert™XC3 includes on-board two/three-way live voice communication technology so that Track Group Monitoring Center operators or authorized County personnel can speak to the participant directly 24/7/365. The device also allows the participant to place a call (via a button on top of the device) directly to the Monitoring Center in cases of emergency.

Additionally, Track Group will provide the County with an allowance of six (6) cell phones to be used by program participants (offenders); any cell phones for program participant use beyond the allowed six (6) cell phones will be charged the rate as designated in the Daily Use Per Unit Cost in the Schedule of Compensation. Track Group will provide an unlimited number of cell phones, as requested by the County, pre-loaded with the Victim Application to program victims per the Schedule of Compensation.

- B. Federal Communications Commission (FCC) compliant and registered.** Track Group's GPS devices comply with the applicable Federal Communications Commission (FCC) regulations and are registered:

Shadow™ (FCC# TPO-MUV2).  
ReliAlert™XC3 (FCC# TPO-OTD36)  
Beacon™ (FCC# TPO-B03)

- C. GPS receiver communicates with U.S. Government Global Positioning System.** Shadow™ and ReliAlert™XC3 technology includes GPS receivers that are capable of receiving information from the U.S. Government Global Positioning System.
- D. Unit operation when in proximity to other GPS/RF receivers or electronic devices.** Shadow™ and ReliAlert™XC3 functionality, communication and locationing technology is not affected by being in the proximity of other GPS/RF receivers and electronic devices; and therefore operates normally in these environments.
- E. Unit collection and transmission of location data as frequently as every minute.** The standard collection and transmission rate for Shadow™ and ReliAlert™XC3 is every minute. Less frequent collection and transmission rates can be implemented if required.
- F. Unit internal clock with date and time stamp of all recorded events.** Shadow™ and ReliAlert™XC3 have on-board, internal clocks and all recorded events are date and time stamped.
- G. Unit recording and storing capabilities of location data (minimum of 48 hours).** Shadow™ is capable of recording and storing 30 days of location, event, violation and device data in the event of a communication disruption; ReliAlert™XC3 is capable of recording and storing 18 days.

The devices consistently search for a cellular connection and once re-established, transmit all stored data automatically to the TrackerPAL™ system and Track Group Monitoring Center. Additionally, if the battery becomes depleted and the device shuts down, all un-transmitted data messages are maintained and then transmitted once the device is restarted and cellular communication is established.

- H. GPS device initial signal acquisition time (no more than five minutes).** Both Shadow™ and ReliAlert™XC3 are able to comply with this requirement.

- I. **Unit safety features; units shall not pose safety hazard.** Shadow™ and ReliAlert™XC3 are FCC-certified not to cause bodily harm by emissions of RF energy. SAR (Specific Absorption Rate) certification requirements ensure that an FCC-approved cellular device operating in near proximity to the human body does not generate energy emissions of levels that could represent health concerns. Design of both devices external chargers and device charging interfaces have been explicitly tested to confirm electrical safety even if electrical contacts are shorted. This includes safety validation for external charger, external electrical contacts and also inclusive of any potential for an internal electrical short such as if shell was compromised in a way that would allow water into the device.
- J. **Device tamper resistance.** Shadow™ has embedded fiber optics in the center of its strap that, if compromised in any way, immediately generates a "Strap Tamper" alert which is sent to the TrackerPAL™ system and Track Group Monitoring Center. Additionally, technology within the device will generate a "Case Tamper" alarm if the device shell is opened.

ReliAlert™XC3's standard strap has dual, braided stainless-steel cables encased in the outer edges. The embedded dual steel cables provide rigidity; prevents the wearer from heating up and stretching the plastic to remove it without severing the strap and makes it cut-resistant. A fiber-optic strand is embedded in the center of the strap that, if compromised in any way, immediately generates an alert which is sent to the TrackerPAL™ system and Track Group Monitoring Center. Additionally, technology within the device will generate a "Case Tamper" alarm if the device shell is opened.

ReliAlert™XC3's optional high-security strap - SecureCuff™ can be used for medium and high-risk participants, in lieu of the ReliAlert™XC3's standard strap. It has an encased, hardened steel 1" band that provide extreme cut-resistance and includes the same fiber-optic technology as the standard strap for tampering notification.

- K. **Device component functionality in normal environmental and atmospheric conditions.** Both Shadow™ and ReliAlert™XC3 are waterproof (40 feet and 20 feet respectively) and capable of functioning in temperatures ranging from -4° Fahrenheit to +143° Fahrenheit.
- L. **Device components shock and vibration endurance capabilities.** Both Shadow™ and ReliAlert™XC3 have been designed and tested to withstand beyond "normal wear and tear" endurance including passing shock-tests and drop-tests.
- M. **Moisture and water-resistant device components.** Both Shadow™ and ReliAlert™XC3 are waterproof (40 feet and 20 feet respectively) and allow the participant to engage in normal activities such as bathing, showering, swimming and sweating.
- N. **Unit's internal diagnostics and ability to relay information.** Shadow™ provides information to detect tampering and spoofing. Additionally, the device includes status bits with all event messages to indicate things like GPS Error, RF Radio error, etc. ReliAlert™XC3 has extensive self-diagnostics to automatically identify and report cellular network service anomalies and device error conditions. It automatically generates statistical data and transmits to server when device encounters issues such as impaired strap optical performance or over-temperature conditions.

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 GPS

Such issues are reported prior to reaching a service impacting level. For conditions not necessitating immediate action, Track Group Monitoring Center reviews Quality-Of-Service reports weekly to identify devices which reflect possible signs of requiring repair or field intervention (e.g. replacement of strap).

- O. **Unit receiver signal unique to assigned individual.** Each Shadow™ and ReliAlert™XC3 has a unique serial number and unique IMEI number, so when a device is assigned to a participant (upon enrollment) within the TrackerPAL™ system, the data reported from the device is linked to the that participant.
- P. **Bracelet component hypoallergenic qualities.** The Shadow™ strap is made up of Hypoallergenic Polyurethane and the rubber over-molding that covers the shell is made of DowCorning thermoplastic elastomer. The ReliAlert™XC3 device is made up of hypoallergenic materials, including Hypoallergenic Polyurethane in the strap (commonly used in medical applications); and Dupont ST 801 in the back-shell.
- Q. **GPS device batteries recharge ability.** Shadow™ includes a charging cord that can be plugged into a standard AC outlet and connected into the bottom of the device. ReliAlert™XC3 includes a charging cord that can be plugged into a standard AC outlet and connected to the front of the device.
- R. **Device battery-operated components' minimum battery life (minimum one year before requiring replacement).** The battery shelf life of both the Shadow™ and ReliAlert™XC3 is greater than two (2) years and the battery-operating life of both is approximately 1.2 years.
- S. **GPS device receives and transmits location data while being charged.** Shadow™ and ReliAlert™XC3 are capable of receiving and transmitting location data, events and alarms while the device is being charged (and powered up); as long as there is a cellular communication connection. There is no change to the standard capturing and reporting of data (every minute) when in a "charging" state.
- T. **Active GPS device time to full charge (should be within 2 hours).** Both ReliAlert™XC3 and Shadow™ can be fully charged within two (2) hours.
- U. **Active GPS receiver will emit low battery warning.** Shadow™ provides up to 48 hours of battery operation and ReliAlert™XC3 provides 55+ hours of operation before shutdown. "Low battery" status is communicated to the participant via vibration and the LED atop each device begins flashing "red." This "low battery" event is transmitted to the TrackerPAL™ software and is viewable by authorized County personnel. When either reaches a "Battery Critical" state, an alert is generated and transmitted to the TrackerPAL™ software and pre-established violation notifications are followed by the system and/or the Track Group Monitoring Center. If charging activities do not occur, eventually a "Battery Critical Escalated" alert is generated and transmitted to the TrackerPAL™ software; at which point, pre-established violation notification protocols are followed by the system and/or Track Group Monitoring Center. Vibration and LED visual notifications continue to be provided to the Participant until charging is initiated and sustained.

- V. **Active GPS receiver will retain stored data when the battery is depleted.** Shadow™ and ReliAlert™XC3 automatically maintain all un-transmitted data if the battery becomes depleted and the device shuts down. When the device is restarted and cellular communication is established, all stored data is transmitted to the TrackerPAL™ system.
  - W. **Active GPS receiver battery operation time (on a single charge) at the maximum levels of location point collection and transmission.** Shadow™ provides up to 48 hours of battery operation at one-minute point collection and transmission on a single battery charge; ReliAlert™XC3 provides 55+ hours and one-minute point collection and transmission.
  - X. **Unit low-battery life warning and time frame.** Track Group's alert provides approximately 90-days' notice prior to battery life end.
  - Y. **Device components physically attach to the participant, sizing structure, portability, and ease of use when engaged in physical activities, including manual labor.** Both Shadow™ and ReliAlert™XC3 are installed on the participant's ankle via sized straps and strap connection pins (Shadow™) and security screws (ReliAlert™XC3). Both devices are ergonomically designed to fit comfortably on the participant's ankle and will not unduly restrict normal or work activities.
  - Z. **Fulfillment of additional units and associate time frame.** Track Group will provide each Department the required 30% shelf stock (on active devices) and all consumables at no cost until activated on a participant. If additional units are requested by a Department, Track Group's local equipment fulfillment center enables delivery of units within 24 hours, including holidays and weekends. All shipping costs are the sole responsibility of Track Group.
- AA. GPS system provides Sheriff's Office, Adult Probation and Juvenile Probation immediate alert notifications.** Alert notification protocols can be established by County authorized personnel, within the TrackerPAL™ software interface, by alarm type. Notification methods include text message, email and live phone call and are either automatically initiated by the TrackerPAL™ system or handled by the Track Group Monitoring Center upon receipt of an alert. Victim notification is also included in the violation notification protocols and includes text message, email or live phone call by the Track Group Monitoring Center.
- BB. Active GPS equipment's location detection accuracy.** The GPS performance specifications of Shadow™ and ReliAlert™XC3 is accurate to within 50 ft. more than 95% of the time in typical field operations, however, performance may vary based upon the environment.
- CC. GPS equipment will utilize a supplemental or an enhanced tracking system when GPS is unavailable or diminished.** Technology within both the Shadow™ and ReliAlert™XC3 ensure that once either device recognizes a loss of the GPS signal, it automatically provides cellular triangulation as a secondary means of tracking – within two (2) minutes for ReliAlert™XC3 and within 10 minutes for Shadow™.

### 2.2.3 Active GPS Software

- A. Central host and software system's accessibility to the Department for a minimum of two hundred (200) simultaneous users.** The TrackerPAL™ software system is web-based and accessible by authorized County personnel (with an authorized username and password) at any time via a computer with high-speed internet. This system is robust and scalable and can easily accommodate an additional 200+ simultaneous users, per agency, with no loss of functionality or performance.
- B. System will track and display all participant information including but not limited to required demographics (including stored participant photo and vehicle information), assigned supervision officer(s); assigned device(s); zones.** Within TrackerPAL™, authorized County users can input and view varying degrees of information on the participant (including all required fields); as well the participants photo, vehicle information, assigned device(s) and assigned officer.

TrackerPAL™ allows authorized County users to create a “protocol set” which involves selecting those alerts that require notification steps; then selecting the method(s) and recipient(s) for the notification. Notifications may either be done automatically by the TrackerPAL™ system (required email and text messages) or via the Track Group Monitoring Center (live phone calls, device audio and vibration commands).

All geo-zones for a specific participant are viewable and editable within TrackerPAL™. Geo-zones can be created in the shape of a circle/oval, square/rectangle or polygon and can be sized and/or moved as needed.

TrackerPAL™ utilizes Google Maps™ mapping technology to provide current and historical tracking of a participant. Tracking points and data are in numerical, sequential order and allow for incremental point by point viewing. Queries can be customized via the selected timeframe. Tracking and inclusion/exclusion zones, shown on the mapping interface, can be printed. Track Group Monitoring Center Staff will utilize the location point of the alert/violation to determine which local law enforcement entity to contact for specific alerts (see below) for the domestic violence cases based upon predetermined protocols from the county agency, and a complete list of appropriate contact numbers for each law enforcement agency. Track Group Monitoring Center staff will place a live phone call to the appropriate law enforcement for the following alerts:

- A stationary exclusion zone violation
- A mobile exclusion zone violation
- A device tamper alert when the Victim cannot be reached or the Victims states that they feel they are in danger.
- Other alerts/events according to predefined Agency protocols.

Agency personnel will provide a complete list of all Cook County law enforcement agencies and the appropriate contact numbers for the Track Group Monitoring Center to use for these events/alerts. Track Group Monitoring Center staff will contact the appropriate Cook County law enforcement agency per the agency defined protocols and make every reasonable effort to contact the appropriate law enforcement agencies outside of Cook County for alerts/events that occur outside of the County.

- C. Software system will display the physical location of the Actively GPS-monitored participant on a user-friendly interactive map containing recognizable state, county, municipality, and street names.** TrackerPAL™ uses Google Maps™ for all mapping activities. Authorized County users can view points of interest icons, tracking information on the map in standard, satellite, hybrid (satellite view with street name overlay), or street view; as well as assigned inclusion/exclusion zones within the mapping area.

All location information transmitted from Shadow™ and ReliAlert™XC3 devices are in longitude/latitude format when received by the TrackerPAL™ software system. The location points plotted on the map in the TrackerPAL™ are based solely on the latitude/longitude coordinates. To obtain the street address shown in the event table, a reverse geocoding feature is automatically engaged to calculate an approximate address.

For every location, event or alarm transmission, Shadow™ and ReliAlert™XC3 provide the following additional device information: event/alarm type, date and time, approximate address, device battery strength, cellular signal strength, number of GPS satellites engaged, alarm status, and the direction and approximate speed of travel. This information is viewable within the mapping screen in an information box. Tracking points plotted on the map reflect the level of confidence in the GPS accuracy – Circle (High), Square (Medium).

- D. Software system's ability to establish and edit exclusion zones, inclusion zones, mobile zones, travel zones, and jurisdictional zones and, buffer zones.** Inclusion and exclusion zones can be created in the shape of a circle/oval, square/rectangle, or polygon and can be manipulated and sized to ensure an accurate location; then designated as an inclusion zone or an exclusion zone. Schedules (days/times) can then be created based upon when participants are required to be within the zone (inclusion zone) or outside the zone (exclusion zone). Created zones and schedules can be easily edited at any time by authorized users. The size and shape of the zones are customizable per participant.

Buffer zones can be created and users have the ability to select the "width" of the buffer zone surrounding the geo-zone. By using the polygon-shaped geo-zone, users can create travel zones (inclusion) for the participant. Jurisdictional zones can also be created by utilizing the polygon-shaped geo-zone to ensure areas like the city, county or state can be defined and applied as an inclusion zone.

Track Group's Victim smartphone application creates a mobile geo-zone around a victim and works in conjunction with the participants GPS tracking device (Shadow™ or ReliAlert™XC3), to provide an early warning notification to the victim when they are in proximity to the participant. Additionally, users can create a customizable sized circular buffer zone around the mobile geo-zone.

- E. Software system's ability to configure multiple schedules for a single participant (e.g., weekday and weekend schedules).** Once a geo-zone is created, users can create a schedule for that zones that involves different days and different hours in a day. Additionally, multiple schedules can be created and saved for any zone for a single participant.

- F. Software system's ability to establish zones for individual GPS-monitored participants and for groups of GPS-monitored participants.** If logged in as an "officer" in the TrackerPAL™ system, users can access any zone created in the officer's "zone library." These zones can be added to any participant's zone library for assignment and activation. If logged in as an "admin" in TrackerPAL™, users can access any zone created by any officer or admin in the system, and then assign them to any participant.

Also, the County can create "public" geo-zones and assign them to a category (for example "Schools"). During participant enrollment that category of zone is assigned the participant. In the future if a new zone is added to that category then the new zone automatically applies to all participants that are linked to that category.

- G. Software system's ability to create polygon shaped zones for GPS-monitored participants.** Within TrackerPAL™, geo-zones can be easily created into a polygon-shape by selecting the polygon icon. Once the shape is plotted onto the map, users can manipulate the shape by clicking and dragging any of the five (5) points of the polygon to create the required shape.
- H. Software system ability to configure alert protocols that are unique to each participant and to configure alert protocols for certain groups of participants.** Within TrackerPAL™, authorized County users can create a "protocol set" which involves selecting those alarms that require notification steps; then selecting the method(s) and recipient(s) for the notification. Notifications may either be done automatically by the TrackerPAL™ system (required email and text messages) or via the Track Group Monitoring Center (live phone calls, device audio and vibration commands) to either the victim, local law enforcement or the supervising agency. Once protocols have been established for the appropriate alarms, users save the protocol set making it available to assign to a participant.
- I. Software system's ability to display the status and history of the required alerts.** All events and alerts are listed (and highlighted) in the Events Grid within the TrackerMap section of the software. Additionally, tracking points that include an alert are represented on the map by a "flashing siren" in lieu of the standard tracking point icon. Users can also "filter" the Events Grid to only reflect alerts within the specified time period so that they can quickly be reviewed. Additionally, users can quickly run an Alarms Detail report that provides details of all alerts associated with one participant or all participants for a period of time. This status and historical display applies to all County required alerts.
- J. Software system ability to view and manage the Department equipment inventory.** Authorized County users are able to view all GPS devices assigned to the County within TrackerPAL™. This device list includes the following: serial #, equipment type, inventory location, assignment status.
- K. Software system's ability to interface with third-party applications and related equipment, including any applicable Jail Management System such as the Sheriff's Jail Management System ("CCOMS"), to provide real-time data synchronization for monitoring and reporting.** Track Group's software system will provide RESTful web services API which can be used by a third party system to push into our system and pull data from it. It is also possible to create a module that

will push data entered into our system to a third party system provided the third party system exposes a web service interface or database connection.

- L. **Software system's ability to print maps of GPS-monitored participant's location points that indicate the accurate date, time and direction of travel.** Authorized users are able to run, save and print a report that includes a map of the tracking timeline selected, as well as a list of the tracking points with the following information: Event Name (GPS Trace, Alarm, Event), GeoRule (if applicable), approximate location, and event date/time. All GPS location information is designated as either being either a "High" or "Medium" confidence location.
  
- M. **Software system's ability to track and display relevant information about the victim where applicable.** Track Group's Victim smartphone application creates a mobile geo-zone around a victim and works in conjunction with the participants' GPS tracking device (Shadow™ or ReliAlert™XC3), providing an early warning notification to the victim when they are in proximity to the participant. Within TrackerPAL™, authorized County users view the current and historical tracking of participants. If there is a victim involved with a participant, and the survivor has opted to download and utilize Track Group's smartphone application, County users can also view the tracking of the victim in the mapping interface. Victim tracking points are white while the associated participants tracking points are red. When requested, Track Group will provide a smartphone preloaded with the Victim App, at the rates set forth in Schedule of Compensation.

#### **2.2.4 Equipment Compliance**

Track Group's GPS devices comply with the applicable Federal Communications Commission (FCC) regulations and are registered:

Shadow™ (FCC# TPO-MUV2).  
ReliAlert™XC3 (FCC# TPO-OTD36)  
Beacon™ (FCC# TPO-B03)

#### **2.3 GPS Monitoring Software**

- 1) **Monitoring software system shall track and display participant information including but not limited to the following: required demographics including stored participant photo and vehicle information), assigned supervision officer(s); assigned device(s); and zones**

Within TrackerPAL™, authorized County users and/or Track Group Monitoring Center personnel can input and view varying degrees of information on the participant (including all required County fields); as well the participants photo, assigned device(s); assigned supervision officer and zones.

Participant tracking points and data are in numerical, sequential order and allow for incremental point by point viewing. Historical queries can be customized via the selected timeframe.

- 2) **Monitoring software system will display the address assigned to the unit on a user-friendly interactive map containing recognizable state, county, municipality, and street names.**

The TrackerPAL™ software uses Google Maps™ for all mapping activities. Authorized users can view points of interest icons, tracking information on the map in standard, satellite, hybrid (satellite view with street name overlay), or street view; as well as assigned inclusion/exclusion zones within the mapping area.

All location information transmitted from ReliAlert™XC3 and Shadow™ devices are in longitude/latitude format when received by the TrackerPAL™ software system. The location points plotted on the map in the TrackerMap tab are based solely on the latitude/longitude coordinates. To obtain the street address shown in the event table, a reverse geocoding feature is engaged to calculate an approximate address.

- 3) **Monitoring software system will configure multiple schedules for a single participant (e.g., weekday and weekend schedules).**

Once a geo-zone is created, users can create a schedule for that zone involving different days and different hours in a day. Additionally, multiple schedules can be created and saved for any zone for a single participant.

- 4) **Monitoring software system will display the status and history of alerts.**

For every location, event or alarm transmission, Shadow™ and ReliAlert™XC3 provide the following additional device information: event/alarm type, date and time, approximate address, device battery strength, cellular signal strength, number of GPS satellites engaged, alarm status, and the direction and approximate speed of travel. This information is viewable within TrackerPAL™ by authorized County users.

All events and alarms are also listed (and highlighted) in the Events Grid within the TrackerMap section of the software. Additionally, tracking points that include an alert are represented on the map by a “flashing siren” in lieu of the standard tracking point icon. Users can also “filter” the Events Grid to only reflect alarms within the specified time period so that they can quickly be reviewed.

Users can quickly run an Alarms Detail report that provides details of all alarms associated with one participant or all participants for a period of time.

- 5) **Monitoring software system will allow the County to view and manage the Department equipment inventory.**

In the inventory section of the software, authorized County users are able to view all GPS devices assigned to the County. This device list that includes the following: serial #, equipment type, inventory location, assignment status. Track Group will provide a 30% shelf inventory (of active devices) Orders for additional devices will be filled within 24 hours

of request, including weekends and holidays. All delivery/shipping costs are the sole responsibility of Track Group

**6) Monitoring software system participant specific reports, inventory reports, and management reports, including participant specific location for GPS monitoring.**

The TrackerPAL™ monitoring software provides multiple "demand" reports available to authorized users 24/7 and include: Activation Report, Inventory Report, Alarm Details Report, Assigned Track Group Report, Back-up Contacts Report, Participant Demographics Report, Daily Alarm Overview Report, Participant Schedules Report, Deactivation Report, Enrollment Report, Monitoring History Report, Most Recent Alarms History Report, Participant Alarm Summary Report. Examples of these reports are included in Exhibit XX. These reports can be exported/downloaded into the following formats: Excel, PDF, Tiff, XML, CSV, and Web Archive.

*Inventory reports* will include, at a minimum and separated by type of device, the total amount of units on the participating Department's premises ready for use, total available to the participating Departments in Track Group's off-site inventory, and total amount of active units currently being used by participants.

*Management reports* shall include, at a minimum, how many units are still in the field subject to retrieval, how many units are still in the field presumed lost or damaged, how many units Track Group is scheduled to pick up and the schedule for retrieval. These reports will be capable of being generated by the participating, authorized Department staff at any time, but at least daily. The system will have the ability to query, sort, and search by any field and generate any reports requested by the Sheriff's Office, Adult Probation, or Juvenile Probation.

*Non-standard reports* will include: Average Length of Stay; Contact Report; Contacts per Watch Report; Count Report; Court Movement Report; Monitored Report; Violations Report; Movement Report; New Arrests Report; New Entries by Day Report; New Release Reject Report; No Hits Report; Participant Report; Participant Charge Report; Participant End Report; Participant End Count Report; Pregnant Report; Program End Report; SR County by Deposition; SIR Number Look Up Report; Violation Count Report; and Work School Hit Report.

**7) Monitoring software system will send participant alerts, violations and equipment malfunctions to the appropriate County department via a dedicated computer dispatch system that will individually track and record information regarding the handling and processing of each incident.**

Shadow™ and ReliAlert™XC3, along with the TrackerPAL™ monitoring system, are capable of recognizing violations and immediately generating automated alert notifications via text and email to designated County personnel and victims based upon pre-established notification protocols. Phone call notification can be made by the Track Group Monitoring Center upon violation notification within the monitoring system alarm queue to local law enforcement,

the using agency and victims— notification is also based upon pre-established notification protocols.

The TrackerPAL™ software interface allows authorized County users to establish violation notification protocols by alarm and then create “protocol sets” that can be applied to any participant. Notification methods include text message, email and live phone call. Notification protocols that only require an email or text message, are automated and immediately sent out once the TrackerPAL™ recognizes the violation or receives the alert from either GPS device.

- 8) **Monitoring software system's case-management component capable of tracking each individual participant's progress while on the program including violations, officer contacts, drug tests, and general observations.**

Track Group's monitoring software system is TrackerPAL™. If necessary and requested by the County, the software can integrate with Track Group's case management software or the County's case management system.

## **2.4 GPS Monitoring Center Service Requirements**

- a) **Monitoring Center will conduct alert analysis and resolution using Department defined protocols.**

Track Group's Monitoring Center maintains a comprehensive Knowledgebase, providing information on Department policies, step by step alert handling procedures approved by the Department, and call handling procedures. Changes or additions to the database are routinely completed with collaboration between the Account Manager, Operations, Training, and the appropriate Department personnel.

This scripting is used in conjunction with the web-based solution developed for each client to ensure all outbound calling steps, text/email notifications and alert follow-up procedures are followed by the Monitoring Center staff. Track Group currently uses live monitoring staff to escalate as well as proprietary online dispatching system developed on the web based solution software for each Department. The online dispatching system, previously described, provides the County with a reliable accountability tool to track and respond to all escalated alerts from the Track Group Monitoring Center.

- b) **Proposer shall provide all data entry services associated with participant enrollments, schedules, activity data, and alert response/notification. Proposers shall propose their plan to provide 24-hours a day staff to enter into a database new participants, participants' violations, schedules and all actions taken by the Sheriff's Office, Juvenile Probation and Adult Probation and Proposer's staff.**

Track Group's Monitoring Center will provide 24/7 staff available to meet and exceed all data entry requirements for each Department as they currently do. This includes all enrollments, schedules, activity data, alert response/notification and additional needs as they arise.

Information can be communicated to the data entry desk via fax, email or phone. Dedicated email addresses can be assigned as needed for each Department. Steps taken to communicate and document data are as follows:

1. Department emails/faxes/phones in request
  2. Correctional Specialist performs data entry
  3. A confirmation email for email requests is sent
  4. Faxed information is entered and noted in the system
- c) **Monitoring Center will provide/maintain and answer a separate toll-free communications network for Sheriff's Office, Juvenile Probation, and Adult Probation personnel.**

Track Group's Monitoring Center will provide and maintain multiple toll free numbers in order to accommodate separate lines for each Department (Sheriff's Office, Adult Probation and Juvenile Probation). Additional lines will be added and designated as required to meet the needs of the County.

- d) **Proposer shall describe how it will offer toll-free access to live technical support personnel, who shall be available 24 hours per day, seven days per week and any integrated voice recognition system it administers to reduce staff time.**

Track Group's Monitoring Center is staffed 24/7, 365 days a year providing technical support, including troubleshooting, event interpretation and application questions, through the toll free number provided at no additional cost to the County. Any questions/concerns that the operator cannot resolve will be escalated to the Supervisor on Duty who is available on every shift. If the issue cannot be resolved within 24 hours, Track Group will provide a written, detailed plan of action to address the issue, including an explanation as to why resolution within 24 hours is not possible. This plan of action will be provided to the Sheriff's Office, juvenile Probation and Adult Probation Departments within two (2) hours.

- e) **On-site technical support, when required.**

Track Group's corporate headquarters is based in the Chicago-Area and has experienced technicians out of this location to ensure that on-site technical support can be provided to the County, same-day, if a problem arises that cannot be corrected by telephone or email. The technician provided will be highly-trained, experienced and familiar with the scope and procedures of this County contract.

- f) **Liaison for the Sheriff's Office, Juvenile Probation Department and for Adult Probation to meet monthly or as needed to discuss contract performance.**

Track Group's liaison for the Sheriff's Office, Juvenile Probation Department and for Adult Probation will be the Director of Account Management. This individual is based out of Track Group's Chicago-Area based office and will be available to meet monthly or as needed to discuss contract performance.

- g) Plan to maintain and repair/replace all equipment leased from Proposer, including repairing equipment in participants' residences, for the duration of the contract at no additional cost to the County.**

Track Group's technicians providing equipment retrievals will also be providing equipment repair and replacement services for the County; in the participants' residence if necessary. If repair efforts do not resolve the issue, the technician will immediately replace the affected device with one from inventory and will return the deficient device to Track Group's fulfillment center for assessment and repair. Additionally, the technician will place an order to have a replacement device shipped to replenish inventory levels.

In the event of a system outage or service interruption that renders the devices and/or system unable to properly monitor program participants, notify victims or process alerts and events Track Group's monitoring center staff will begin its outage notification procedures. Agency staff and County personnel will be immediately notified of a system outage via text and/or email message within 15 minutes after the Track Group Monitoring Center is aware of an outage. Additionally, Track Group Monitoring Center staff will place live operator phone calls to designated Agency/County staff to inform of the issue. Program Victims will be immediately notified of a system outage via text and/or email message within 15 minutes after the Track Group Monitoring Center is aware of an outage. Track Group Monitoring Center staff will place live operator phone calls to all impacted victims within a timely manner utilizing all available Track Group Monitoring Center staff to inform them of the system outage. Track Group Monitoring Center staff will then notify Agency/County personnel and all impacted victims once the system outage is cleared or restored.

Track Group agrees to be responsible for all equipment shipping and receiving costs. Once Track Group staff are notified through the agreed upon transmittals that an offender has completed the program or should be removed from the program, the offender will be deactivated from the system and a retrieval order will be initiated. Once the notification has been received to remove the client from the program, the equipment (inventory) assigned to that offender will be removed from the Agency inventory upon system deactivation and shall not count against the Agency's shelf allowance pending retrieval or drop-off.

- h) Plan for fulfilling the County's request for additional devices within twenty-four (24) hours (including weekends and holidays).**

Track Group will provide each Department the required 30% shelf stock (on active devices) at no cost until activated on a participant, so that inventory is readily available if needed. If additional units are requested by a Department, Track Group's local fulfillment center and enables delivery of units within 24 hours. Track Group is responsible for all equipment shipping and receiving costs.

- i) Inventory allowance (a minimum of an additional 30%) for Department of the total number of units that are in use, without any fee.**

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 GPS

Track Group will provide the County with a 30% inventory allowance for the Sheriff's Office, Juvenile Probation and Adult probation, based upon the total number of active units. Devices that fall under the inventory allowance percentage are not billed until activated on a participant.

**j) Providing testimony, at no additional cost, regarding the performance and methodologies of Track Group's equipment and services**

Track Group will immediately notify the County on receipt of any subpoena involving or affecting the GPS Monitoring Equipment and Services contract and will work with judicial officers and judiciary entities to provide pertinent information and instruction in the manner and use of its equipment and services.

Additionally, and upon request by the Sheriff's Office, Juvenile Probation, Adult Probation and/or court, Track Group will provide an individual to meet any testimony requirements.

**k) Plan to instruct participants on the use and care of the equipment.**

Track Group will provide all necessary training/user guides for the proposed equipment, applications and systems in written and video format for the proposed equipment and systems. These guides include instructions for both officers and participants on the use and care of the equipment.

**l) Plan to provide its employees who will provide services under this contract written policies and procedures in order to ensure compliance with the requirements in this Request for Proposals.**

Track Group will conduct mandatory staff meetings to present the full scope of the County contract to include the contracts written policies and procedures required to be followed for full contract compliance. Ongoing training and meetings will also be held on a frequent basis to ensure that all policies and procedures are continually reviewed with all staff. Track Group will also continue presenting all County policies, procedures and approved protocols during our extensive training sessions.

**m) Manage retrieval of all monitoring equipment from Participants following notification from the County of program completion.**

Track Group and the County Departments will agree to an equipment retrieval notification process; as well as the timeframe expectations for retrieval upon notification. Track Group's team of technicians will be trained on this process and will be responsible for GPS equipment retrieval, 24/7/365, for the County. Whether the agreed upon notification of a participant program completion is a phone call or email to the designated Track Group department, Track Group will immediately log the retrieval request information into the system database and the request information is dispatched to the team of mobile technicians. Once the technician receives the retrieval request, the request is added to his/her schedule. Upon equipment retrieval, the technician logs receipt of the equipment and maintains ownership until delivered

back to the appropriate Department location. Every effort is made to retrieve the equipment in a timely timeframe agreed to help minimize against equipment loss.

Track Group billing for the County will cease at 12:00am CST on the day that the County notifies Track Group of a participant's program completion. Once Track Group staff are notified through the agreed upon transmittals that an offender has completed the program or should be removed from the program, the offender will be deactivated for the system and a retrieval order will be initiated. Once the notification has been received to remove the client from the program, the equipment (inventory) assigned to that offender will be removed from the Agency inventory upon system deactivation and shall not count against the Agency's shelf allowance pending retrieval or drop-off.

- n) **Track Group shall accept all phone calls from participants, compile all required paperwork including court orders, work schedules, paystubs, appointment letters and immediately forward any and all movement permission requests or emergencies to Sheriff's Office personnel via their dedicated computer system.**

Track Group's Monitoring Center offers a fully staffed 24/7, 365 day operation to be able to assist the Sheriff's office with all of its needs. This additional level of case management and monitoring service shall also be available to Adult Probation should Adult Probation elect to utilize the additional service. The Track Group Monitoring Center utilizes an online web based solution that assists in documentation of all inbound and outbound calls, data entry requests, and permission requests. All emergencies or serious incidents will be documented and escalated via phone call to the Sheriff Dispatch office immediately. In addition, all information gathered by the Track Group Monitoring Center via phone call, fax or email is immediately uploaded to the web based solution and will be available for viewing/retrieval by the Sheriff's office. The Track Group Monitoring Center is also able to customize and expand the storing and sharing of data for the Sheriff's office as requested. This additional level of Case Management and Monitoring Service is available to both the Sheriff's Office program and the Adult Probation Program per the Schedule of Compensation.

- o) **Protect against failure of central host system and software.**

Track Group's *Disaster Recovery Plan* is in place to ensure that there is no or limited interruption of the Department's program, and in the event of a catastrophe, all information is safely stored and recovered. At the most basic level, Track Group utilizes the following features to ensure continuity of operations under adverse conditions on a day-to-day basis:

- *Redundant Server Architecture.* All of Track Group's monitoring computer systems employ multiple redundancies. Track Group's server architecture continuously copies all data from the primary server to a separate redundant server so both servers contain the same data at the same time. If a component of our architecture fails, a redundant component will automatically come online. Track Group's dual-server architecture provides a layer of isolation if repairs are needed or if localized outages occur.

- *Uninterrupted Power Supplies (UPS)*. The primary computer room is supported by a dual-UPS system. Each server is equipped with two power supplies and receives backup power from both UPS systems. This design minimizes the downtime associated with a single UPS failure. The UPS and generators are maintained and tested on a regular basis to ensure proper functionality.

### **Site Description**

#### *Primary Data Center*

The primary Track Group Data Center is located in Dallas, TX. The facility is a one story building with concrete and raised floors. The data center cage is approximately 300 Sq. ft., contains primary and secondary power to all racks, entire facility uninterruptible power supply (UPS) protection backed by multiple power generation systems using diesel and turbine powered generators. Data center utilizes BGP backed Internet connections to ensure access to Internet facing applications.

#### *Backup Data Center and Primary Monitoring Center.*

The backup Track Group Data Center is located Aurora, IL. The facility is a single story building with concrete floors and a raised computer room floor. Office contains primary operations workstations, backup mission critical servers and UPSs. The backup data center is collocated with a full contact operations center composed of approximately 100 stations.

#### *Backup Monitoring Center*

The backup Monitoring Center for Track Group is in Anderson, IN. The facility is single story building with dual UPS systems that feed power to the computer room and all Monitoring Center PCs. Facility is backed up by redundant diesel generators and can run on a single generator. There are two diverse data entrances with 50' of separation. The facility contains approximately 100 workstations.

### **Prevention**

*Generator:* Generators are located at the primary and backup sites to power the entire data centers. The Dallas generators run on diesel and other fuels and can run indefinitely as long as fuel is replenished. The Aurora, IL backup generator operates from natural gas and can run indefinitely. All generators are under maintenance contracts and they are load tested annually. Auto-transfer switches are configured to start the generator within ten seconds of a power failure.

*Uninterruptible Power Supplies (UPS):* UPS units are configured between our generators and all mission critical computer systems (servers, switches, and routers). All mission critical systems are powered through dedicated circuits. The UPS systems hold power long enough for the generators to power up and take the load.

*Disk and Tape Backup Systems:* The Data Center performs differential backups to disk on mission critical systems daily with full backups on Sundays. Information to be archived for long term storage is sent to tape. Tapes are not reused and are stored offsite. The Track Group Data Center will use a similar disk backup solution as well as tape, which are picked up every Monday via courier, same schedule as the primary data center. The disk backup data is replicated

between sites for easy retrieval at any of the 3 locations; Dallas, TX, Aurora, CO and Anderson, IN.

*Cabling/Switches:* All cabling is rated at CAT5 and CAT6, allowing for fast speeds that cut down on interference. Primary data center uses Dell layer 3 switches and backup centers utilize Cisco, 3-layer switches. Virtual Local Area Networks (VLANS) are configured to provide more efficient traffic flow.

*Router/Firewall:* All three locations utilize Sophos UTM firewalls with Full Guard licensing that perform deep packet inspection and web filtering. All are setup in a high available protocol (HA) configuration so that if one should fail, the other will immediately pick up and route traffic between the Internet, demilitarized zone (DMV) and internal networks. All three locations are connected via a VPN-backed MPLS network.

*Internet Connection:* The Internet connection at the primary data center utilizes public internet protocol (IP) addresses on a BGP-backed Internet connection. This provides access to public facing applications through multiple Internet providers. Track Group's Internet access is provided by a fiber last mile connection through Century Link, and the Anderson Call Center uses both Level3 and CenturyLink Internet connections that are controlled via the unified threat monitor (UTM) firewalls.

*Servers/Operating System:* Unless redundancy is already employed, such as in a server web farm, all critical servers have dual redundant, hot swap power supplies and RAID-5 redundant hard drive systems. We have made efforts to use the same hardware (primarily Dell) when possible to provide for parts swapping in a disaster situation. Our servers run primarily on Windows 2008 and 2012r2 operating systems in a multi-domain environment. The IT department leverages the system centers operations manager (SCaM) application for primary server monitoring as well as custom scripts that check for possible upcoming and immediate problems that require attention.

*Antivirus:* We utilize the Sophos Antivirus application at all facilities. Local installations can be pushed from a local server at each location. Virus detection files are updated automatically multiple times a day. Regular virus scans are scheduled to run nightly. Automatic email virus detection is employed. Servers are in a continuous scanning mode for optimal protection.

*Desktops:* Track Group primarily uses equipment from Dell and the equipment is locked down via a Microsoft Active Directory domain. Minimal access is a security requirement for all three facilities and is enforced through the AD domain controllers.

All PCs run the Sophos AV clients.

*Premise Security:* Access to the primary data center is tightly controlled through the use of personalized proximity cards to enter the building, and a personalized door code to get into the data center itself. A cage code and a card reader on the data center stage are also required for entry. Any access to the primary data center cage is reported on an ongoing basis to a team of managers and network security personnel. Personalized proximity card access is required at all locations to enter the facilities and computer room access.

*Telecom:* The Track Group interactive voice response (IVR) systems are redundant between the Dallas, TX and Aurora, IL data centers. Each IVR is fully licensed and can receive and process calls simultaneously. If a change is made to an IVR at the Track Group location, the changes are updated automatically to the IVR at the other data center. The Avaya systems support all three locations, and interact with a common set of core functions but are able to fully standalone and process calls in the event of a disaster. Avaya phone systems is supported by 24x7 4 hour response maintenance contracts. IVR calls, which require a customer to speak with an agent, can be worked out of any of the call centers.

## 2.5 GPS Information System Requirements

### General

- a) **Central host system and software system and its accessibility to the Sheriff's Office, Juvenile Probation and Adult Probation via the Internet through a standard web-browser interface.**

TrackerPAL™ is accessed via a standard web interface, with an authorized username and password. This system is robust and scalable and can easily accommodate an additional 2300+ simultaneous users, per agency, with no loss of functionality or performance.

- b) **Web-based monitoring host and server/monitoring system and all necessary components that will actively monitor, check, and verify that participants remain in their residence during specific time periods and shall report unauthorized absences, late returns, equipment malfunctions or any and all alerts that may be construed as program violations.**

TrackerPAL™ is a secure, web-based application that receives, records, and stores all data transmitted from Shadow™ and ReliAlert™ XC3 devices. Inclusion and exclusion zones, with schedules, can be created and edited in the system; and then activated on the appropriate participants' device. The system, in conjunction with the GPS devices, actively "monitors and verifies" if the participant is following the appropriate schedule as it relates to each geo-zone and an alert is generated if geo-zone parameters are not followed. The GPS devices and systems also provide alert notification for issues like battery power, tampering, loss of communication, loss of GPS, etc.

TrackerPAL™ also provides users with the ability to input/view/edit participant demographic information, officer assignment, images uploads, viewing of current and historical tracking information, creating geo-zones/schedules, running reports

- c) **All messages and information entered and/or recorded in this host server shall be permanently recorded and easily accessed by authorized personnel of Track Group, Adult Probation, Juvenile Probation and Sheriff's Office personnel.**

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 GPS

TrackerPAL™ is a secure, web-based application that receives, records, and stores all data transmitted from Shadow™ and ReliAlert™ XC3 devices. All information received from Track Group's electronic monitoring products are permanently recorded within the system. Additionally, information entered by authorized County users regarding the participant, schedules, zones, etc. are also permanently recorded. The secure, robust system is accessible by authorized personnel from Track Group, Adult Probation, Juvenile Probation and the Sheriff's Office, 24/7/365 from any computer with a high-speed Internet connection with no additional hardware or software needed.

**d) System's capability to provide accurate real-time counts of active participants as well as accessible archived data for past program participants.**

The Home page of TrackerPAL™ allows users to view a current listing of all participants within the program and their status: a "green" status is an assigned and active participant; a "yellow" status is an assigned and inactive participant; and a "red" status is an inactive participant.

Within the Inventory section of TrackerPAL™, users can view the current status of all devices and the associated participant (if applicable) – a "green" status is an assigned and active device; a "yellow" status is an assigned and inactive device; a "red" status is an unassigned device and a "black" status is a device that is in RMA. Additionally, users can run an Agency Device Inventory report provides the total number of devices that are "active," "inactive" and in "RMA."

Once a device is activated, all participant information, including personal information, tracking points, alarms, etc. is stored in TrackerPAL™ and can be accessed 24/7 by authorized County personnel. Information is readily available via the software on all active participants; as well as inactive participants, for 18 months. If a participant has been inactive for more than 18 months, information is archived to storage for an additional 5 ½ years or until the contract terms dictate. Archived information on a participant can be requested and it will be provided within 48 hours.

**e) Mobile data terminal units (Toughbooks) or tablets to be provided to the Sheriff's Office, Juvenile Probation and Adult Probation.**

Track Group agrees to provide the following additional equipment to the County:

- 20 mobile data terminals – Sheriff's Office
- 25 tablets – Juvenile Probation
- 20 tablets – Adult Probation

Track Group will provide wireless service for Adult and Juvenile Probation Departments' mobile terminal units or tablets. The Sheriff Department will be responsible for wireless service on their equipment.

- f) **Offsite remote access to the host system capabilities allowing for viewing, editing, reports, and queries.**

The secure, web-based TrackerPAL™ software interface is accessible by authorized County personnel at any time via a computer with high-speed internet access and receives, records, and stores all data transmitted from ReliAlert™XC3 and Shadow™ devices. Depending upon the assigned user role, authorized County users can log in and view, edit, generate reports and run historical tracking queries.

- g) **Format the monitoring system will send participant alerts, violations and equipment malfunctions to the Sheriff's Office, Juvenile Probation and Adult Probation.**

Violation notifications sent by the TrackerPAL™ system have the same message format:

**Track Group Alarm Notification**

Participant: Grant Demo

Alarm: Inclusion Zone Violation

Date/Time: 10/25/2016 at 1:40 PM.

Zone: HOME

Officer: Grant Law

Additionally, the Track Group monitoring platform will also process compliance notifications indicating an alert/event has been resolved for those alarms/events that possess the compliance notification feature.

- h) **Monitoring system's case management capabilities for tracking each individual participant's progress while on the program including violations, officer contacts, drug tests, and general observations.**

Track Group's monitoring software system is TrackerPAL™. If necessary and requested by the County, this software can integrate with Track Group' case management software or the County's case management system.

- i) **The Sheriff's Office facilitates and maintains booking, release, movement, classification, and all related records for each detainee in its custody by way of the Sheriff's Jail Management System (hereinafter "CCOMS"). Adult Probation and Juvenile Probation intend to create similar management information systems in the future. The Sheriff and all Participating Agencies therefore require real-time data synchronization with CCOMS or related systems for monitoring and reporting in order to reduce data entry and eliminate errors.**

Track Group's software system will provide RESTful web services API which can be used by a third party system to push into our system and pull data from it. It is also possible to create a module that will push data entered into the system to a third party system provided the third party system exposes a web service interface or database connection.

- j) Confirm and identify that the monitoring system and software will successfully interface with, CCOMS and related systems, including Adult Probation's and Juvenile Probation's future management information system(s). This interface shall include real-time data synchronization and the ability to exchange data for the Participating Agency's access and use.

Track Group's software system will provide RESTful web services API which can be used by a third party system to push into the system and pull data from it. It is also possible to create a module that will push data entered into our system to a third party system provided the third party system exposes a web service interface or database connection.

## 2.6 Data Security and Compliance

Security structure and process used by the solution to provide access control to the application and all related data from a web interface. Solution's information reliability and security standards. Software and database security features. In particular, the County requires user-defined privileges, authentication, network and database security modules, and information sharing security (e.g., encryption, user-defined privileges, legal considerations (including those related to probation records and HIPAA), auditing concerns, mechanisms for tracking access and updates, and interface interactions).

### 2.6.1 Security Structure and Process

Track Group's security structure and process includes:

#### User Security

- *Authentication:* User data on our database is logically segregated by account based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on.
- *Passwords:* User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- *Single Sign-On:* For our Team Collaboration accounts, Track Group supports SAML 2.0 integration, which allows you to control access to the system across your organization and define authentication policies for increased security.
- *Data Encryption:* Certain sensitive user data, such as participant details and account passwords, are stored in encrypted format.
- *Data Portability:* Track Group enables you to export your data from our system in a variety of formats so that you can back it up, or use it with other applications.
- *Privacy:* We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.
- *Data Residency:* All Track Group user data is stored on servers located in the United States.

#### Physical Security

All Track Group information systems and infrastructure are hosted in world-class data centers. These data centers include all the necessary physical security controls you would expect in a data center these days (e.g., 24x7 monitoring, cameras, visitor logs, entry requirements). Track Group has dedicated cages to separate our equipment from other tenants. In addition, these data centers are SOC 2 accredited.

### **Availability**

- *Connectivity:* Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.
- *Power:* Servers have redundant internal and external power supplies. Data centers have backup power supplies, and are able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.
- *Uptime:* Continuous uptime monitoring, with immediate escalation to Track Group and Agency staff for any downtime.
- *Failover:* Database is replicated in real-time and can failover in less than an Hour.
- *Backup Frequency:* Backups occur daily at multiple geographically disparate sites.

### **Network Security**

- *Testing:* System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.
- *Firewalls:* Firewalls restrict access to all ports except 80 (http) and 443 (https).
- *Access Control:* Secure VPN, 2FA (two-factor authentication), and role-based access is enforced for systems management by authorized engineering staff.
- *Logging and Auditing:* Central logging systems capture and archive all internal systems access including any failed authentication attempts.
- *Encryption in Transit:* By default, our system has Transport Layer Security (TLS) enabled to encrypt respondent traffic. All other communications with the system are sent over TLS connections, which protects communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients. Our application endpoints are TLS only and score an "A" rating on SSL Labs' tests. We also employ Forward Secrecy and only support strong ciphers for added privacy and security.

### **Vulnerability Management**

- *Patching:* Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.
- *Third Party Scans:* Environments are continuously scanned using best of breed security tools. These tools are configured to perform application and network vulnerability assessments, which test for patch status and basic misconfigurations of systems and sites.
- *Penetration Testing:* External organizations perform penetration tests at least annually.
- *Bug Bounty:* Track Group runs a private bug bounty program to ensure our applications are continuously reviewed for vulnerabilities.

### **Organizational & Administrative Security**

- *Information Security Policies:* Track Group maintains internal information security policies, including incident response plans, and regularly review and update them.
- *Employee Screening:* Track Group performs background screening on all employees, to the extent possible within local laws.
- *Training:* We provide security and technology use training for employees and agencies.
- *Service Providers:* We screen our service providers and bind them under contract to appropriate confidentiality and security obligations if they deal with any user data.
- *Access:* Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.
- *Audit logging:* We maintain and monitor audit logs on our services and systems.

### **Software Development Practices**

- *Stack:* We code in Python and run on SQL Server, Windows, and Ubuntu.
- *Coding Practices:* Our engineers use best practices and industry-standard secure coding guidelines, which align with the OWASP Top 10.
- *Deployment:* We deploy code dozens of times during the week, giving us the ability to react quickly in the event a bug or vulnerability is discovered within our code.

### **Compliance and Certifications**

- *PCI:* Track Group is currently PCI 3.1 compliant.
- *HIPAA:* Track Group offers enhanced security features that support HIPAA requirements. See below.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States law that regulates the collection and handling of "protected health information" (PHI). Certain organizations called "covered entities" and their business associates are required to comply with HIPAA.

For Track Group, being "HIPAA-compliant" means that we offer a service that enables covered entities to collect and manage PHI through monitoring in a manner compliant with HIPAA. As part of offering this service, Track Group ensures that it operates in a way that is consistent and compatible with those laws and Track Group's role as a business associate to a covered entity user.

**Procedures (e.g., background checks, hiring practices, etc.) for ensuring Track Group employees are properly authorized for access to confidential and sensitive participant information. Practices for training Monitoring Center employees and for ensuring they are properly qualified to handle confidential and sensitive information. Track Group shall ensure that the confidentiality of participants' records is maintained and shall not disclose any such information to any third party without written authorization of the County. Data generated as a result of monitoring shall not be used in any way by Track Group without consent of the Department.**

All employee applications are thoroughly evaluated by our Human Resources Director and assessed based upon the experience and skill set of an individual against the job positions' functional

requirements and education. All employee candidates, at Track Group, must have a high school diploma or a GED and their reasons for leaving previous jobs are also taken into consideration.

Once an individual has been identified as a candidate they must pass a state and federal background check (that includes criminal history for up to seven years); a 5-panel drug-test; along with verification of eligibility to work in the U.S. before being offered the position. Once the results of all checks and tests are received and approved, the individual is hired. New hire training is customized based upon the job position and can include both "classroom" and "hands-on" training depending on the responsibilities.

Track Group policies govern the confidentiality of customer information and data. In addition to the policies and procedures regarding records release, employees must sign a confidentiality agreement before being hired. Within Track Group's policies and procedures, unauthorized disclosure of information is prohibited and will not occur without written request by authorized County personnel. Track Group will immediately notify County upon receipt of any subpoena involving or affecting this contract. Original documentation will not be released unless required by court subpoena; otherwise, photocopies will be provided. Data generated as a result of monitoring shall not be used in any way by the Proposer without consent of the Department.

**Ability to create user groups with varying access privileges (e.g., read/write and read only).**

The TrackerPAL™ software has three User Roles to allow agencies to limit user functionality:

- *Agency Admin* – has access to all agency/participant information and full functionality within the TrackerPAL™ system; as well as the ability to edit agency information and add agency users to the system.
- *Officer* – has access to their officer and participant information only; with full functionality within the TrackerPAL™ system under this constraint.
- *Admin Assistant* – has "view-only" functionality for all agency-participant information within the following interface tabs: Home, Participant Info, My Info and Reports.

**Each participant's data shall be accessible to the Participating Agency for a minimum of 18 months before it is archived or stored offline, from the end of the service.**

TrackerPAL™ is a secure, web-based application that receives, records, and stores all data transmitted from the ReliAlert™XC3 and Shadow™ devices. This information is readily available via the software on all active participants as well as inactive participants for 18 months. If a participant has been inactive for more than 18 months, the participants information is archived to storage for an additional 5 ½ years or until stated by the contract terms. Archived information on a participant can be requested and it will be provided within 48 hours. At the end of the contract period, Track Group will provide the County all event/history/archived data related to the contracted GPS monitoring products and services.

**Archived copies of each participant's data shall be retained for a minimum of 5 years. Upon expiration of the retention period and/or termination of the Agreement, the awardee must facilitate transfer of all participant data and related records created in performance of the Agreement.**

Track Group will securely maintain archived copies of the County's participant data for a minimum of five (5) years and upon expiration of the retention period and/or Contract termination, will facilitate a transfer of all participant data and related records generated in the Contract performance to the Participating Agency in an easily stored and interpreted format.

**Location of the central host system, the repository of all monitoring data, which shall not be located in a County's facility and shall be the responsibility of Track Group.**

Track Group's TrackerPAL™ application resides on an IBM secured and redundant system in Dallas, TX. The IBM System is SSAE 16, ISO 27001, SOC2 and Safe Harbor Compliant and the Infrastructure covers redundant networking, power and Infrastructure. These systems are monitored by IBM Managed Services 24 hours, seven days a week; augmenting Track Group's IT team in ensuring that the physical environment is both stable and secure. The location is hardened against physical intrusion, and server room access is limited to certified employees. All of controls (inside and outside the data center) are vetted by third-party auditors.

Access to the TrackerPAL™ monitoring interface can be determined by authorized County officials. Those officials assigned an "Admin" user role in TrackerPAL™ are the only ones within the County that can add other authorized users to access the County's participant information within TrackerPAL™.

## **2.6.2 Data Security Controls**

**Overview of the System's software, hardware, and other controls supporting the System's data security.**

Track Group's security structure and process includes:

### **User Security**

- *Authentication:* User data on our database is logically segregated by account based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on.
- *Passwords:* User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- *Single Sign-On:* For our Team Collaboration accounts, Track Group supports SAML 2.0 integration, which allows you to control access to the system across your organization and define authentication policies for increased security.
- *Data Encryption:* Certain sensitive user data, such as participant details and account passwords, are stored in encrypted format.
- *Data Portability:* Track Group enables you to export your data from our system in a variety of formats so that you can back it up, or use it with other applications.
- *Privacy:* We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

- *Data Residency:* All Track Group user data is stored on servers located in the United States.

### **Physical Security**

All Track Group information systems and infrastructure are hosted in world-class data centers. These data centers include all the necessary physical security controls you would expect in a data center these days (e.g., 24x7 monitoring, cameras, visitor logs, entry requirements). Track Group has dedicated cages to separate our equipment from other tenants. In addition, these data centers are SOC 2 accredited.

### **Availability**

- *Connectivity:* Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.
- *Power:* Servers have redundant internal and external power supplies. Data centers have backup power supplies, and are able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.
- *Uptime:* Continuous uptime monitoring, with immediate escalation to Track Group and Agency staff for any downtime.
- *Failover:* The database is replicated in real-time and can failover in less than an Hour.
- *Backup Frequency:* Backups occur daily at multiple geographically disparate sites.

### **Network Security**

- *Testing:* System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.
- *Firewalls:* Firewalls restrict access to all ports except 80 (http) and 443 (https).
- *Access Control:* Secure VPN, 2FA (two-factor authentication), and role-based access is enforced for systems management by authorized engineering staff.
- *Logging and Auditing:* Central logging systems capture and archive all internal systems access including any failed authentication attempts.
- *Encryption in Transit:* By default, the system has Transport Layer Security (TLS) enabled to encrypt respondent traffic. All other communications with the system are sent over TLS connections, which protects communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients. The application endpoints are TLS only and score an "A" rating on SSL Labs' tests. We also employ Forward Secrecy and only support strong ciphers for added privacy and security.

### **Vulnerability Management**

- *Patching:* Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.
- *Third Party Scans:* The environments are continuously scanned using best of breed security tools. These tools are configured to perform application and network vulnerability assessments, which test for patch status and basic misconfigurations of systems and sites.
- *Penetration Testing:* External organizations perform penetration tests at least annually.

- *Bug Bounty:* Track Group runs a private bug bounty program to ensure our applications are continuously reviewed for vulnerabilities.

#### **Organizational & Administrative Security**

- *Information Security Policies:* Internal information security policies, including incident response plans are maintained, and regularly reviewed and updated.
- *Employee Screening:* Background screenings are performed on all employees, to the extent possible within local laws.
- *Training:* Security and technology use training is provided for employees and agencies.
- *Service Providers:* Service providers are screened and bound under contract to appropriate confidentiality and security obligations if they deal with any user data.
- *Access:* Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.
- *Audit logging:* Audit logs on our services and systems are maintained and monitored.

#### **Software Development Practices**

- *Stack:* Coding is in Python and run on Sal Server, Windows, and Ubuntu.
- *Coding Practices:* Track Group engineers use best practices and industry-standard secure coding guidelines, which align with the OWASP Top 10.
- *Deployment:* Track Group deploys code dozens of times during the week, giving us the ability to react quickly in the event a bug or vulnerability is discovered with in our code.

#### **2.6.3 Compliance and Certifications**

- *PCI:* Track Group is currently PCI 3.1 compliant.
- *HIPAA:* Track Group offers enhanced security features that support HIPAA requirements. See below.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States law that regulates the collection and handling of "protected health information" (PHI). Certain organizations called "covered entities" and their business associates are required to comply with HIPAA.

For Track Group, being "HIPAA-compliant" means that we offer a service that enables covered entities to collect and manage PHI through monitoring in a manner compliant with HIPAA. As part of offering this service, Track Group ensures that it operates in a way that is consistent and compatible with those laws and Track Group's role as a business associate to a covered entity user.

Track Group confirms that all instances of Track Group software serving the US market are hosted in the US.

#### **2.6.4 Incident Response Requirements**

**Approach to meeting data security incident response requirements:**

Track Group's Incident Response Plan (IRP) provides instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats as well as procedures for documentation. This plan enables Track Group to respond quickly and effectively. Our IRP plan covers several phases: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned and identifies the names, contact information and responsibilities of the response team.

**a. Maintenance of the Proposers' Incident Response Plan;**

Track Group's Director of Operations and Information Technology is responsible for maintaining our Incident Response Plan and reviewing the Plan every six (6) months.

**b. Conformance of such plan to Illinois Personal Information Protection Act and the breach notification laws of the fifty states;**

Track Group's Incident Response Plan conforms to the Illinois Personal Information Protection Act and the breach notification laws of the fifty states.

**c. Cook County's rights of review, approval and reasonable modification to Proposer's incident response plan;**

Upon request, Track Group will provide a formal copy of Track Group's Incident Proposal Plan to the County for review and approval. Should the County suggest reasonable modifications to the Plan, Track Group will review the modification requests against Track Group's internal and external Plan requirements and determine if such modifications can be implemented.

**d. Approach to provide detailed reports on the nature of incidents and identified data lost or stolen;**

Track Group learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under various state and federal laws and regulation, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or phone calls if a breach occurs.

**e. Plan to address security incidents and data breaches in alignment with the following requirements. For events within the control of Track Group, Track Group is expected to:**

**i. Immediately notify the County of incidents and breaches;**

Working in conjunction with the County, Track Group will develop and implement a specific communication procedure to be followed to ensure immediate notification to the County of an incident or breach.

**ii. Identify immediate plan of action to mitigate further incident progression;**

Track Group's incident response team works quickly to analyze and validate each incident, following the Incident Response Plan's pre-defined process. When an incident occurs, an initial analysis is immediately conducted to determine the scope, i.e. which systems are affected, how the incident is occurring and if possible, who or what originated the incident. This initial analysis is critical and allows the team to better prioritize containment activities and next steps for a deeper analysis of the incident.

**iii. Identify protection measures for affected individuals;**

After the initial incident analysis is completed by Track Group's incident response team, appropriate protection measures for affected individuals will be implemented.

**iv. Provide outbound and inbound incident-related communications, as requested and directed by the County**

Track Group will work with the County to develop and implement a notification and communications procedure, both outbound and inbound, regarding incident-related communications.

### **2.6.5 Business Continuity and Recovery**

#### **Methodology to perform system upgrades and maintenance during times typically associated with low volumes of system use.**

The TrackerPAL™ application is updated regularly through maintenance releases and major releases, which contain new features and feature changes. Maintenance releases can occur as frequently as every month and generally last 15 minutes or less. Major releases typically occur once a quarter and may require up to a 30 minute maintenance window. Servers are kept patched as needed.

Maintenance and major releases are typically scheduled during timeframes where the least amount of activity is occurring in the TrackerPAL™ application.

#### **Average amount of downtime needed to accommodate the System availability tiers described below.**

The TrackerPAL™ application is updated regularly through maintenance releases and major releases, which contain new features and feature changes. Maintenance releases can occur as frequently as every month and generally last 15 minutes or less. Major releases typically occur once a quarter and may require up to a 30 minute maintenance window.

Track Group agrees to provide notice to the County in advance of any scheduled maintenance or upgrades and will provide written details regarding the interruption.

**Unanticipated service interruptions - incident notification plan and communication methodology to immediately notify the Sheriff's Office, Juvenile Probation and Adult Probation.**

Following any service interruption, Track Group will follow-up with Sheriff's Office, Juvenile Probation and Adult Probation by submitting a report within 24 hours that includes the following:

- The ticket number along with a description of the event;
- The start and end times of the service interruption;
- An explanation of how the contractor became aware of the problem;
- Affected systems and users;
- Non-affected systems and users;
- Prevention methods implemented to avoid recurrence; and
- Required action by the Sheriff's Office, Juvenile Probation and Adult Probation, if any.

**Automated backup and recovery capability for the system and application, including incremental and full back-up capabilities.**

**Availability**

- *Connectivity*: Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.
- *Power*: Servers have redundant internal and external power supplies. Data centers have backup power supplies, and are able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.
- *Uptime*: Continuous uptime monitoring, with immediate escalation to Track Group and Agency staff for any downtime.
- *Failover*: Track Group's database is replicated in real-time and can failover in less than an hour.
- *Backup Frequency*: Backups occur daily at multiple geographically disparate sites.

**Ability to provide the service from at least two geographically diverse data centers that do not share common threats (e.g. the data centers cannot be in the same earthquake zone, likely hurricane path, same flood zone, etc.). The data centers must at a minimum meet Tier III standards for redundancy of power, telecommunications, HVAC, security, fire suppression and building integrity.**

Track Group's two data centers are geographically diverse and do not share common disaster threats. Each center has meets minimum Tier II standards for power redundancy, telecommunications, HVAC, security, fire suppression and building integrity.

**Implementation of crisis management, business continuity, and disaster recovery plans.**

Track Group has a situation-based plan that includes clear roles, responsibilities and process-related organizational requirements company-wide. The plan addresses action with regards to crisis prevention, crisis assessment, crisis handling and crisis termination and helps Track Group ensure a rapid and

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 GPS

adequate response to any crisis, clear lines of reporting and communication in the event of crisis and agreeing rules for crisis termination.

Track Group's business continuity planning (BCP) defines the potential risks, identifies how the risks will affect operations and then implementing safeguards and procedures designed to mitigate the risks. Testing is done on these procedures to ensure they work and semi-annual review of the process is done to make sure everything is up-to-date.

Track Group's information technology disaster recovery plan (IT DRP) was developed in conjunction with its business continuity plan. Priorities and recovery time objectives for information technology were developed during the business impact analysis. Technology recovery strategies were developed to restore hardware, applications and data in time to meet the needs of the business recovery. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. Therefore, Track Group has a robust plan for data backup and restoration of all electronic information.

**System will meet the following availability tiers, which tier, and must specifically describe how their system meets such tier:**

Category	Availability	RTO	Characteristics & RPO
High Availability	99.982%	Intra-day	Typically involves data replication to a hot-site for each transaction or at short intervals, like 15 minutes.
Standard Availability	99.741%	24 to 48 Hours	Nightly tape backups shipped to a warm-site data center. System reestablished at time of disaster from tape. May lose up to one day of data.
Non-Critical Availability	99.671%	48 to 96 Hours	Nightly tape backups shipped to offsite warm or cold site data center. System reestablished at time of disaster from tape

Track Group recognizes the importance of data backup and recovery and as such, has initiated the following backup layers to ensure the highest probability of data recovery:

- Level 1 : Transaction Logging of our data to a backup every 5 minutes
- Level 2: Nightly, full backups of our data

- Level 3: Secure, off-system, nightly backups of our data

These backup layers give us a Recovery Point Objective (RPO) of 5 minutes incrementally to 24 hours full.

**System's proven recovery time objective (RTO) and recovery point objective (RPO) in case the primary site becomes unavailable.**

The Veeam Availability Report gathers insights from 1,140 senior IT decision makers (ITDMs) across 24 countries, to develop global network availability standards.

**Key Findings:**

- Unplanned downtime:
  - 1.9 hours for mission-critical applications
  - hours for non-mission-critical applications
- The average recovery time objective (RTO)\*
  - 3.0 hours for mission-critical applications
- The average recovery point objective (RPO)\*\*
  - 4.2 hours for mission-critical applications

\*RTO is defined as time set for resumption of product, service or activity delivery after an incident.

\*\*RPO is the maximum tolerable period in which data might be lost.

According to Veeam Availability Report, organizations encounter unplanned downtime, on average, 13 times per year. Total downtimes above 1 % per year or worse can be regarded as unacceptable as this means a downtime of more than 3 days per year.

**Available performance credits offered for a failure to meet uptime, RTO and RPO requirements.**

Track Group is aware that adjustments for failure to provide satisfactory levels of service may be invoked based on our failure to maintain the requirements and services requested in this Contract and agrees that penalties may be assessed for the following reasons:

- Failure to notify the Sheriff's Office, Juvenile Probation and Adult Probation of participant violations alerts, or inaccurate participant counts.
- Failure to maintain adequate equipment inventory.
- Failure to provide requested reports.
- Failure to provide adequate training for Track Group' staff directly assigned to the County's contract, Sheriff's Office, Juvenile Probation or Adult Probation personnel.
- Failure to perform any of the RFP or contract terms, which results in significant impairment of the monitoring services.

Track Group agrees that the amount of the penalty shall be a minimum of \$1.00 up to the total cost of the daily participant fee per affected participant per day. Performance penalties shall not be applied

before written notice is given from the Sheriff's Office, Juvenile Probation or Adult Probation to Track Group and a review process acceptable to the Sheriff's Office, Juvenile Probation, Adult Probation and Track Group shall be developed once the contract is awarded.

**Each participant's records must be accessible for a minimum of eighteen (18) after completion of monitoring before it is archived or stored offline. Archived copies of each participant's records shall be retained for a minimum of five (5) years after the participant's completion of monitoring and/or provided in a format that can be stored and easily interpreted.**

Participant records in the TrackerPAL™ system and can be accessed 24/7 by authorized County personnel. This information is readily available via the software on all active participants as well as inactive participants for 18 months. If a participant has been inactive for more than 18 months, that participant's information is archived to storage for an additional 5 ½ years or until stated by the contract terms. Archived information on a participant can be requested and it will be provided within 48 hours. At the end of the contract period, Track Group will provide the County all event/history/archived data related to the contracted GPS monitoring products and services.

## **2.6.6 Auditing Requirements**

- a. Track Group will provide SOC 2, Type 2 reports to the County annually or upon request;**
- b. Track Group will provide corrective action plans or actions taken to resolve any exceptions, material weaknesses and/or control deficiencies identified in the SOC report.**

Track Group's Director of Operations and Information Technology is responsible for Service Organization Controls, which include the security of our system; processing integrity of the system; availability of the system; privacy of personal information collected and retained; and the confidentiality of the information the system processes and maintains. This responsibility extends to ensuring correction action plans or actions are taken to resolve any exceptions, material weaknesses, and/or control deficiencies identified in the SOC report.

- c. The County will have the right to access and audit Track Group's system and hosting;**

Track Group agrees to allow the County, upon formal written request, access to our audit system and hosting.

- d. The County will have the right to request reasonable adjustments at Track Group's expense where those requests are based upon audit findings pertaining to the System or Hosting.**

After review of Track Group's audit system and hosting; along with the provided SOC 2, Type 2 reports, the County may contact Track Group with requests for reasonable adjustments to be made to the system or hosting. Track Group will take these requests under advisement and if they don't impact overall Company requirements, will make the adjustments at our own expense.

### **2.6.7 Transition Out and Exit Requirements**

**All data is available to the Sheriff's Office, Juvenile Probation and Adult Probation in an agreed upon format in the event the contract is terminated or contract term expires.**

Track Group agrees to ensure all data is available to the Sheriff's Office, Juvenile Probation and Adult Probation in an agreed upon format in the event the contract is terminated or the contract term expires.

**Exit and transition-out protocols and strategies, including participant equipment transfer, and data retention and transfer.**

Track Group will work with the County and its Departments, along with the new vendor, with regards to participant equipment transfer. Recommendations will be made regarding participant scheduling and maximum daily volume of equipment swap-outs to ensure effective use of both Participant and County staff time and energy. Track Group's equipment retrieval specialists will be on-hand to assist Department staff with removal of Track Group participant equipment. During this time, Track Group will also provide an inventory manager to collect, account for and ship all removed equipment and accessories, along with all shelf inventory at each Department.

All County participant information, including personal information, tracking points, alarms, etc. is stored in TrackerPAL™ and information is readily available on all active participants; as well as inactive participants, for 18 months. If a participant has been inactive for more than 18 months, information is archived to storage for an additional 5 ½ years or until the contract terms dictate.

Track Group will work with the County to provide all County participant monitoring data to the County in the agreed upon medium. Additionally, and upon request by the County, Track Group will work with the County and new vendor (if applicable) to provide the appropriate data transfer of participant data.

**Upon termination of the contract and/or County request, destruction of County data, including backups and copies thereof, as directed by the County.**

Track Group agrees to securely maintain and store all GPS data for the contract term and upon contract expiration/termination, will make the data available to the Sheriff's Office, Juvenile Probation and Adult Probation in an agreed-upon format.

Based upon formal request from County, along with formal indemnification in writing from the County with regards to the destruction of County data, Track Group will destroy the County's data, including backups and copies.

## **3. TRAINING**

***Plan to provide, at no additional cost to the County, on-site training for the Sheriff's Office staff, Juvenile Probation, Adult Probation staff, and other agency personnel in all topics necessary for the implementation and operation of the monitoring system to the full capacity intended by the Sheriff's Office and Adult Probation. The Sheriff's Office, Juvenile Probation and Adult Probation shall choose the dates and locations of the training for their respective agencies. Training shall minimally cover the***

following: installation and removal of equipment; participant enrollment; schedule creation and modification; use of the monitoring system and software; troubleshooting; alert notification protocols, and, any other areas deemed necessary by the Sheriff's Office, Juvenile Probation or Adult Probation. The training shall be delivered by knowledgeable and experienced persons certified by Track Group as subject matter experts and shall include the provision of detailed, written instructions for the participants. Training shall occur prior to implementation, annually for booster sessions, and additionally as requested by Sheriff's Office, Juvenile Probation and Adult Probation when it is required to properly implement and operate the monitoring program (e.g., when new equipment or software is introduced, when there is a major change in County personnel, or when there is an ongoing problem that could be addressed through additional training).

Approximately 265 number of officers/staff may be trained at the County-designated training facility. Approximately 15-20 number of officers/staff may be trained during all different shifts.

Track Group will provide the Sheriff's Office, Juvenile Probation and Adult Probation staff, along with other designated County personnel, with on-site training on all topics necessary for the implementation and operation of the proposed monitoring system. The training will be provided by Track Group's knowledgeable and experienced, Chicago-area training specialists who are certified as "subject matter experts." All training will include detailed, written instructions for the trainees on all three shifts.

Track Group will work with each County Department to schedule the trainings and modify the agenda to best fit each Departments' needs. Track Group's team, resources and experience will ensure that all initial staff training for all Departments will be completed within four (4) weeks; assuming the County can provide at least three training sites for concurrent, weekly training.

#### **4. BILLING CALCULATION**

Billing and payments for program populations will be charged as the actively monitored participant population at 12:00 a.m. (Central Standard Time). Billing and payment must be per participant per day and billed monthly. Monthly invoices must clearly distinguish separate daily active program participant counts by the Sheriff's Office's Department of Corrections, Electronic Monitoring Program and Adult Probation. Invoices must be formatted in the following manner and separated by Department:

Track Group agrees to the program population billing at 12:00am CST and that billing and payment must be per participant per day and billed monthly. Track Group's invoice to the County will distinguish separate daily activities by the three Departments and the invoices will be formatted in the manner set forth in this RFP.

#### **5. PERFORMANCE**

Adjustments for failure to provide satisfactory levels of service may be invoked based on Track Group's failure to maintain the requirements and services requested in this Contract. Penalties may be assessed for the following reasons:

- a) Failure to notify the Sheriff's Office, Juvenile Probation and Adult Probation of participant violations alerts, or inaccurate participant counts.
- b) Failure to maintain adequate equipment inventory.
- c) Failure to provide requested reports.
- d) Failure to provide adequate training for Contractor or Sheriff's Office, Juvenile Probation or Adult Probation personnel.
- e) Failure to perform any of the RFP or contract terms, which results in significant impairment of the monitoring services.
- f) The amount of the penalty shall be a minimum of \$1.00 up to the total cost of the daily participant fee per affected participant per day.

**Performance penalties shall not be applied before written notice is given from the Sheriff's Office, Juvenile Probation or Adult Probation to the Contractor. A review process acceptable to the Sheriff's Office, Juvenile Probation, Adult Probation and the Contractor may be developed once the contract is awarded.**

Track Group understands that performance penalties may be assessed by the County for the above reasons and will work with the County, upon contract award, to develop and implement a "Review Process" for performance penalties.

## 6. Contract Schedule

Event	Responsible Party	Timeline
Contract Commencement	County & Track Group	1/28/2019
Contract Kick-off Meeting	County & Track Group	+ 2 business days
Approval of Training & Implementation Plans	County & Track Group	+ 4 business days
System Integration Complete	County & Track Group	+ 66 business days
Customized Software Development Completed	Track Group	+ 56 business days
County Staff Training Completed	Track Group	+ 14 business days
Offender Data Transition Completed	Track Group	+ 16 business days
Equipment Transition / Deployment Completed	Track Group	+ 30 business days

**NOTE: See Exhibit 1 for Technical Specifications**

**Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS**

**Exhibit 1 to Statement of Work**

**Technical Specifications**

# The safest and most reliable monitoring device ever made.



ReliAlert XC3™ is the only GPS device with **patented 3-way interactive voice communication** that works like a mobile phone attached to the offenders leg.

Track Group's patented **SecureCuff™** helps address the critical "strap cut" issue so prevalent in juveniles and high-risk adult offenders. It significantly reduces the number of officer response hours attempting to locate offenders who have absconded and is not offered by any other service provider.

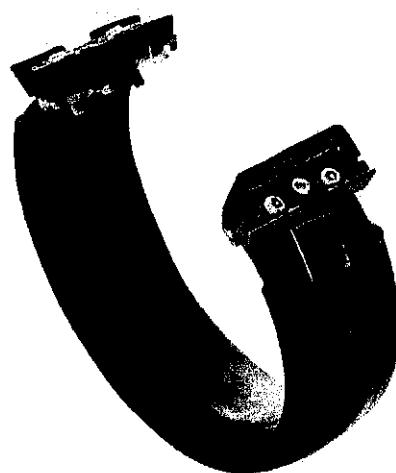
Introducing ReliAlert™XC3 and SecureCuff™

**TRACK**  
GROUP

# Technical Specifications

## RELI ALERT™XC3 SPECIFICATIONS

- **GPS Operation:** updates location and assesses compliance every 2 seconds
- **GPS Accuracy:** 6ft (1.8m) in optimal conditions; within 50ft (15m) under normal operating conditions
- **GPS Anti-Jamming:** advanced, adaptive digital filtering (25 db improvement over conventional GPS receiver)
- **On-Board Processing:** zones and curfews stored on-device are assessed for compliance every 2 seconds
- **Secondary Locationing Technology:** cellular triangulation utilized automatically when GPS is unavailable
- **Battery Performance:** 50+ hours of operation at one-minute tracking and reporting intervals
- **Battery Life:** 500 recharge cycles
- **On-Board Voice Communication:** two/three-way, live voice communication available at any time
- **Siren:** 95 db, activated via software by Monitoring Center or agency users
- **Memory Storage:** approximately 18 days at one-minute tracking and reporting intervals
- **Multiple Monitoring Levels:** available via the software - no equipment change required
- **Tracking/Reporting Interval:** configurable to one or five minutes
- **Embedded RF Technology:** works in conjunction with RF Beacon
- **Alerts:** voice, siren, LED, vibration, audio tones
- **Anti-Tamper Capability:** strap and case tamper technology
- **Standard Strap:** pre-sized and cut-resistant with fiber-optics for tamper detection
- **SecureCuff™:** extremely cut-resistant with encased hardened steel band and fiber-optics for tamper detection
- **Waterproof:** IP68 Certified to 20ft (6m)
- **Operating Temperatures:** -4 to +140 F (-20 to +60 C)
- **Cellular:** 65m and UMTS 3G HSPA+, able to transmit data and SMS during voice calls



## Advanced Features Include

### TWO/THREE-WAY VOICE COMMUNICATION

allows Track Group operators and agency officers to call the offender via the ReliAlert™XC3 device at any time – providing real-time violation intervention and reducing the effort spent by officers attempting to communicate with offenders.

### ONBOARD 95-db SIREN

is a unique feature on the ReliAlert™XC3 device that can be activated by the Track Group Monitoring Center as part of a violation protocol. The siren alerts victims and the public to an offender violation, helps safely assist officers with offender recovery and improves public safety.

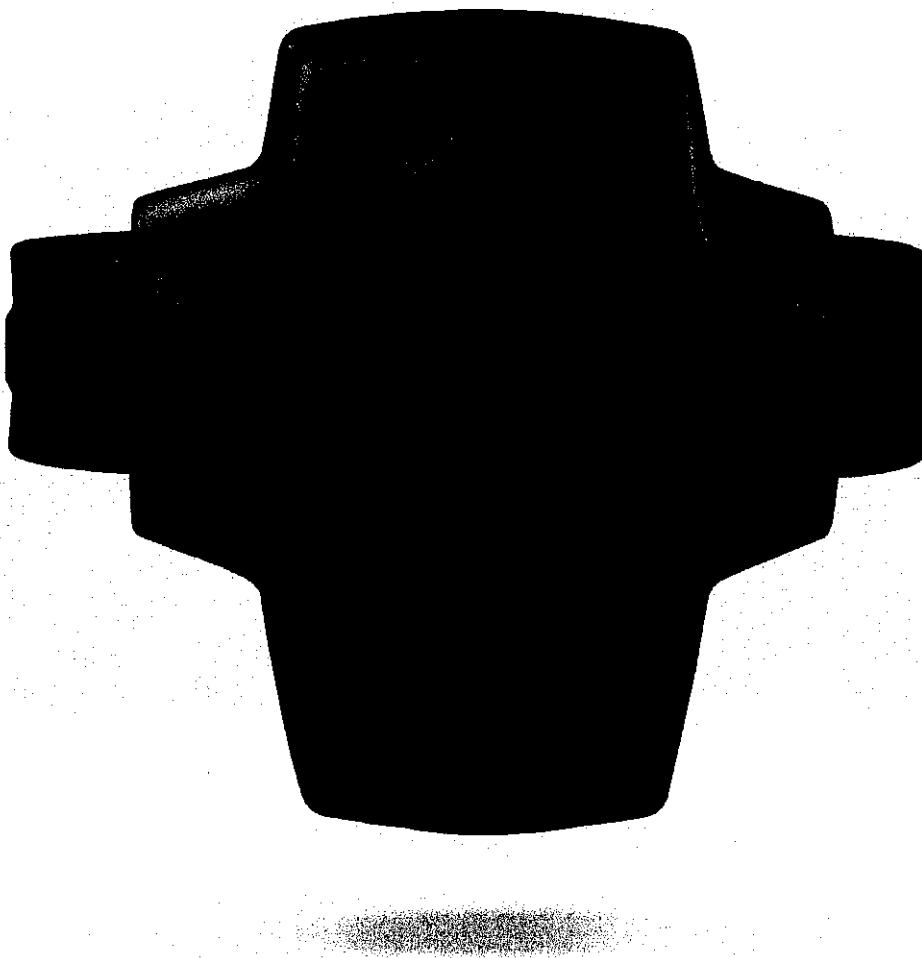
### SECURECUFF™

is an optional, patent-pending, hardened steel encased security cuff for high-risk offenders. The SecureCuff™ provides valuable, extra response time for officers when offenders are attempting to abscond. When used in conjunction with live voice intervention, ReliAlert™XC3 becomes the premier GPS solution for monitoring challenging offender populations.

Introducing ReliAlert™XC3 with SecureCuff™  
See it at [trackgrp.com](http://trackgrp.com)

**TRACK**  
GROUP

The world's smallest, lightest and most  
precise 3G offender tracking device.



Driven by customer demand to improve the performance and affordability of offender tracking devices, Shadow™ is the smallest and lightest device of its kind with a sleek, modern design featuring an enhanced mobile charging capability that makes it easier to use. The device is 3G compliant and fully supported by all global mobility providers.

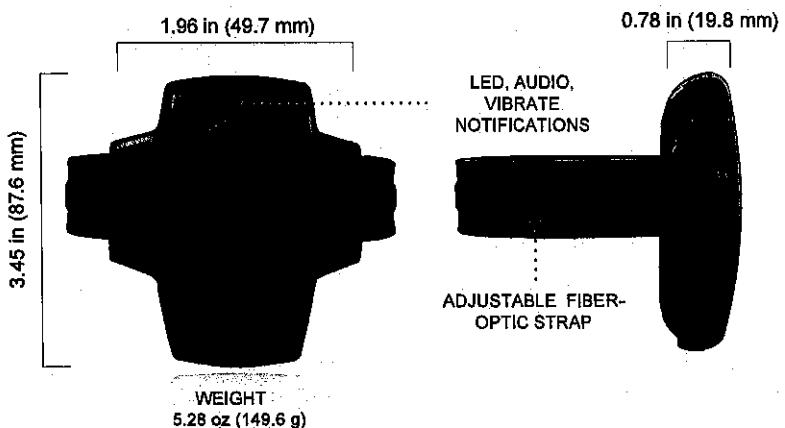
Introducing Shadow™  
See it at [trackgrp.com](http://trackgrp.com)

**TRACK**  
GROUP

# Technical Specifications

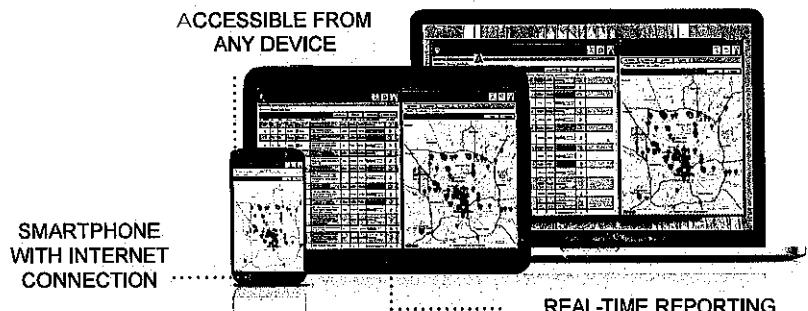
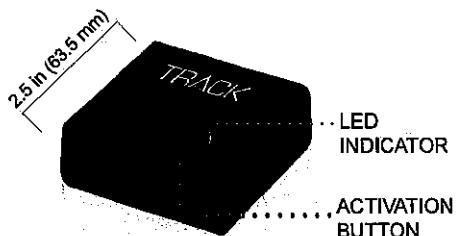
Shadow™ provides seamless and automatic monitoring, enabling routine activities, whether the offender is indoors or outdoors. The complete system includes a tracking device, a beacon and the monitoring platform. The tracking device is small and lightweight and designed to be worn on the offender's ankle incorporating both RF home detention and GPS tracking capabilities in a single unit.

The monitoring platform is a secure cloud-based system that collects, analyzes and displays data from the device.



## TRACKING DEVICE

- Two tracking modes in the same device: continuous RF monitoring indoors and GPS tracking outdoors
- Supports the simultaneous reception of signals from the GLONASS and GPS
- Supports Assisted GPS (A-GPS) to improve start-up performance (time-to-first-fix) and enhance quality and precision when in poor satellite signal conditions
- Cellular triangulation utilized automatically when GPS is unavailable
- Adjustable, tamper-resistant, fiber optic strap with state-of-the-art tamper detection technology
- Case tamper technology
- Fast and easy installation
- Rechargeable battery that lasts up to 72 hours in RF mode and 40-55 hours when used for GPS tracking
- Waterproof (IP68 Certified) to 40 ft.
- Memory storage of approximately 30 days at one-minute tracking/reporting
- Can be paired with up to 5 beacons
- Complies or exceeds global Government requirement specs for EM equipment
- Can be linked with mobile phone application as part of Track Group's domestic violence system



## RF BEACON

- 3.2 oz and 2.5" x 2.5" x 1.0" in size (100gm and 6.35 x 6.35 x 2.54cm).
- Continuous RF monitoring
- Motion detection
- Three (3) year battery operation life
- Battery alarm
- No phone line required
- No external power required
- Can be paired with an infinite number of Shadow™ devices

## MONITORING PLATFORM

- One interface for RF home monitoring and GPS tracking programs
- Remote upgrade and configuration of equipment
- Automatic notifications via SMS and email to pre-defined distributions lists
- Flexible and customizable reporting of locations and violations
- Multilingual

Introducing Shadow™  
See it at [trackgrp.com](http://trackgrp.com)

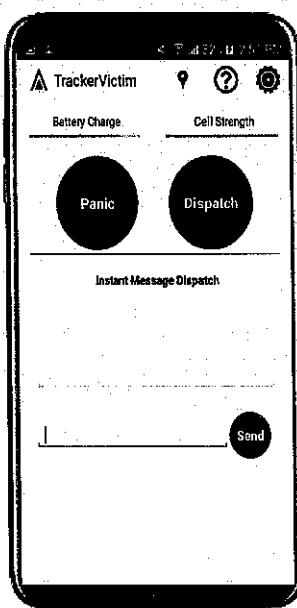
**TRACK**  
GROUP

# Domestic Violence Application

## Integrated Smartphone System

Introducing the first, and only smartphone application that creates a "mobile" geo-zone around a victim and works in conjunction with the offenders tracking device to provide a reliable, early warning notification to the victim when they are in close proximity to the offender.

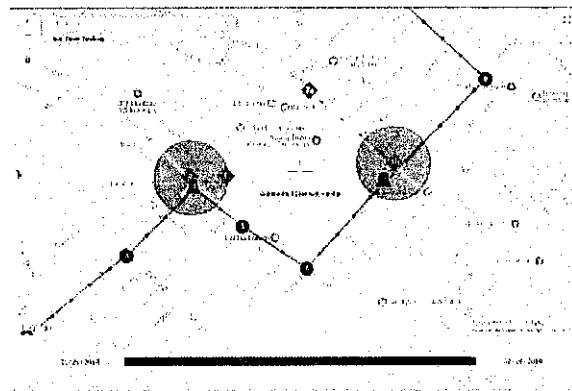
**SIMPLE & EASY TO USE**  
What makes this system unique is that the victim is only required to carry a smartphone with the app installed. The app provides location tracking and communicates with Track Group's system; as well as enabling direct communication with Track Group's monitoring center and law enforcement.



### SPECIFICATIONS

- **Data Communication:** victim location, device and alarm information is transmitted via the victim's cellular carrier or Wi-Fi
- **Data Storage:** app stores location and alarm information if data communication is lost (amount of storage is dependent upon the smartphone). Data is transmitted to Track Group's system once communication is restored
- **Tracking/Reporting Intervals:** once per minute
- **Panic Button:** sends an alarm to the Track Group monitoring center and system; and initiates an outbound call to a configured phone number
- **Dispatch Button:** initiates an outbound call to a configured phone number

Once the app is installed, it communicates automatically with Track Group's system and syncs the smartphone with the offender's tracking device; activating the "mobile zone" created by Agency officers. This zone moves with the smartphone and an alert is generated if the offender breaches the zone parameters.



Introducing Domestic Violence Application  
See it at [trackgrp.com](http://trackgrp.com)

**TRACK**  
GROUP

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 2

Schedule of Compensation

Contract No. 1515-15006B Electronic Monitoring Services  
 Category 2 - Global Positioning System (GPS) Monitoring Equipment  
 Exhibit 2: Schedule of Compensation

<b>GPS Device (LEASED) For Adult Probation</b>	<b>No. Units</b>	<b>Daily Per Unit Cost</b>	<b>Days in Contract</b>	<b>Total Cost</b>
<b>ReliAlert™ XC3 with 2-way voice and standard strap</b> <i>Equipment:</i> ReliAlert XC3 GPS device with 2-way voice and standard strap <i>Services:</i> One-minute tracking and reporting, real-time alarm reporting, customizable alarm notification protocols, alarm notification via email, text message and live phone call, proposed monitoring center services	350	\$3.68	1095	\$1,410,360.00
<b>Victim Services:</b> Access to the domestic violence application, real-time alarm reporting, customizable alarm notification protocols, alarm notification (for victim, officer, and law enforcement) via email, text message and live phone call, proposed monitoring center services	350	\$2.00	1095	\$766,500.00
<b>Victim Equipment:</b> Consultant will provide a supported cell phone for use of the domestic violence application for those Victims who do not have a supported cell phone. (Up to 125 phones is expected, but the number may increase/decrease based on Judicial orders)	125	\$2.00	1095	\$273,750.00
				<b>3 year total</b> \$2,450,610.00

<b>GPS Device (LEASED) For Sheriff's Office</b>	<b>No. Units</b>	<b>Daily Per Unit Cost</b>	<b>Days in Contract</b>	<b>Total Cost</b>
<b>ReliAlert™ XC3 with 2-way voice and standard strap</b> <i>Equipment:</i> ReliAlert XC3 GPS device with 2-way voice and standard strap <i>Services:</i> One-minute tracking and reporting, real-time alarm reporting, customizable alarm notification protocols, alarm notification via email, text message and live phone call, proposed monitoring center services	90	\$3.68	1095	\$362,664.00
Additional Case Management and Monitoring Center Services	90	\$1.45	1095	\$142,897.50
				<b>3 year total</b> \$505,561.50

Contract No. 1515-15006B Electronic Monitoring Services  
 Category 2 - Global Positioning System (GPS) Monitoring Equipment  
 Exhibit 2: Schedule of Compensation

<b>GPS Device (LEASED) For Juvenile Probation</b>	<b>No. Units</b>	<b>Daily Per Unit Cost</b>	<b>Days in Contract</b>	<b>Total Cost</b>
<b>ReliAlert™ XC3 with 2-way voice and standard strap</b> <i>Equipment:</i> ReliAlert XC3 GPS device with 2-way voice and standard strap <i>Services:</i> One-minute tracking and reporting, real-time alarm reporting, customizable alarm notification protocols, alarm notification via email, text message and live phone call, proposed monitoring center services	275	\$3.68	1095	\$1,108,140.00
				<b>3 year total</b> \$1,108,140.00

	<b>Overall Contract Amount</b>	<b>\$4,064,311.50</b>
--	--------------------------------	-----------------------

Neither the County nor any Using Department makes any guarantee as to the number of individuals that may be monitored or the length of time each participant may be monitored. Track Group shall provide services regardless of the actual number of participants or length of time for each participant. County shall pay the equipment and/or services daily rate only for those devices/services that are activated and/or requested by the County.

<b>Accessories:</b>	<b>Daily Per Unit Cost</b>
SecureCuff	Included where indicated above
RF Beacon	Included
ReliAlert XC3 Standard Strap	Included
Power Cord	Included
Break Away Cable	Included
Tamper Caps	Included
Measuring Tool	Included
Torque Driver	Included
Torque Driver Adapter	Included
Driver Bit	Included
Shadow Device	Included
Shadow AC Adapter	Included
Shadow Cable	Included

Contract No. 1515-15006B Electronic Monitoring Services  
 Category 2 - Global Positioning System (GPS) Monitoring Equipment  
 Exhibit 2: Schedule of Compensation

Shadow Locking Pins	Included
Shadow Strap	Included
Mobile Data Terminals (Sheriff's Office) Qty: 20	Included
Tablets* (Juvenile Probation) Qty: 25	Included
Tablets* (Adult Probation) Qty: 20	Included

**\*Track Group will provide wireless service for Adult and Juvenile Probation Departments' mobile terminal units or tablets. The Sheriff Department will be responsible for the wireless service of their equipment.**

System Interface Costs	Cost
Interface Cost for Sheriff's Jail Management System	Included
Interface Cost for Adult Probation Case Management System	Included

Additional Services/Equipment Offered	Daily Per Unit Cost
<b>ReliAlert XC3™ with 2-way voice and SecureCuff™</b> <i>Equipment:</i> ReliAlert XC3 GPS device with 2-way voice and SecureCuff <i>Services:</i> One-minute tracking and reporting, real-time alarm reporting, customizable alarm notification protocols, alarm notification via email, text message and live phone call, proposed monitoring center services	\$3.90
<b>Shadow™</b> <i>Equipment:</i> Shadow GPS device <i>Services:</i> One-minute tracking and reporting, real-time alarm reporting, customizable alarm notification protocols, alarm notification via email, text message and live phone call, proposed monitoring center services	\$3.58
<b>Additional Offender Equipment:</b> Consultant will provide County with an allowance of six (6) cell phones to be used by offenders, any cell phones for offender use beyond the allowed six (6) cell phones will be charged the rate as designated in the Daily Per Unit Cost	\$2.00
Additional Case Management and Monitoring Center Services	\$1.45

Contract No. 1515-15006B Electronic Monitoring Services  
Category 2 - Global Positioning System (GPS) Monitoring Equipment  
Exhibit 2: Schedule of Compensation

<b>Monitoring Center</b>	<b>Daily Per Unit Cost</b>
Proposed Monitoring Center Services	Included where indicated above
Optional Additional Case Management and Monitoring Center Services (Sheriff's Office, Adult Probation)	\$1.45

<b>Application Software</b>	<b>Price Per Month</b>
TrackerPAL™ Mobile Application	Included where indicated above
Analytics (optional package for all 3 programs)	\$12,500.00

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 3

Minority and Women Owned Business Enterprise Commitment



## OFFICE OF CONTRACT COMPLIANCE

**JACQUELINE GOMEZ**

DIRECTOR

118 N. Clark, County Building, Room 1020 • Chicago, Illinois 60602 • (312) 603-5502

Revised May 24, 2018

**TONI PRECKWINKLE**

PRESIDENT

Cook County Board  
of CommissionersRICHARD R. BOYKIN  
1st DistrictDENNIS DEER  
2nd DistrictJERRY BUTLER  
3rd DistrictSTANLEY MOORE  
4th DistrictDEBORAH SIMS  
5th DistrictEDWARD M. MOODY  
6th DistrictJESUS G. GARCIA  
7th DistrictLUIS ARROYO, JR.  
8th DistrictPETER N. SILVESTRIS  
9th DistrictBRIDGET GAINER  
10th DistrictJOHN P. DALEY  
11th DistrictJOHN A. FRITCHY  
12th DistrictLARRY SUFFREDIN  
13th DistrictGREGG GOSLIN  
14th DistrictTIMOTHY O. SCHNEIDER  
15th DistrictJEFFREY R. TOBOLSKI  
16th DistrictSEAN M. MORRISON  
17th District

May 8, 2018

Ms. Shannon E. Andrews  
Chief Procurement Officer  
118 N. Clark Street  
County Building-Room 1018  
Chicago, IL 60602Re: Contract No. 1515-15006B  
Electronic Monitoring Services  
Adult Probation, Sheriff's Office, Juvenile Probation

Dear Ms. Andrews:

The following bid for the above-referenced contract has been reviewed for compliance with the Minority- and Women-owned Business Enterprises (MBE/WBE) Ordinance and have been found to be responsive to the ordinance.

Bidder: Track Group, Inc.  
Contract Value: \$4,064,311.50  
Contract Goal: 25% MBE, 10% WBE

MBE/WBE	Status	Certifying Agency	Commitment (Direct)
Allpoint Security and Detective, Inc.	MBE (6)	City of Chicago	12%
	Total		12%

**Partial MBE and Full WBE Waiver Granted:** Due to the specifications and necessary requirements for performing the contract make it impossible or economically infeasible to divide the contract to enable the contractor to utilize MBES and/or WBEs in accordance with the applicable participation.

The Office of Contract Compliance has been advised by the Requesting Department that no other bidders are being recommended for award. Revised MBE/WBE forms were used in the determination of the responsiveness of this contract.

Sincerely,

*Jacqueline Gomez*Jacqueline Gomez  
Contract Compliance Director

JG/ate

Richard Sanchez, OCPO  
Matthew Sobieski, Adult Probation  
John Webb, Sheriff's Office  
Arnulfo Salazar, Juvenile Probation

Enclosures: Revised MBE/WBE Forms

## MBE/WBE UTILIZATION PLAN - FORM 1

BIDDER/PROPOSER HEREBY STATES that all MBE/WBE firms included in this Plan are certified MBEs/WBEs by at least one of the entities listed in the General Conditions – Section 19.

I. **BIDDER/PROPOSER MBE/WBE STATUS:** (check the appropriate line)

- Bidder/Proposer is a certified MBE or WBE firm. (If so, attach copy of current Letter of Certification)
- Bidder/Proposer is a Joint Venture and one or more Joint Venture partners are certified MBEs or WBEs. (If so, attach copies of Letter(s) of Certification, a copy of Joint Venture Agreement clearly describing the role of the MBE/WBE firm(s) and its ownership interest in the Joint Venture and a completed Joint Venture Affidavit – available online at [www.cookcountylt.gov/contractcompliance](http://www.cookcountylt.gov/contractcompliance))
- Bidder/Proposer is not a certified MBE or WBE firm, nor a Joint Venture with MBE/WBE partners, but will utilize MBE and WBE firms either directly or indirectly in the performance of the Contract. (If so, complete Sections II below and the Letter(s) of Intent – Form 2).

II.  Direct Participation of MBE/WBE Firms  Indirect Participation of MBE/WBE Firms

**NOTE:** Where goals have not been achieved through direct participation, Bidder/Proposer shall include documentation outlining efforts to achieve Direct Participation at the time of Bid/Proposal submission. Indirect Participation will only be considered after all efforts to achieve Direct Participation have been exhausted. Only after written documentation of Good Faith Efforts is received will Indirect Participation be considered.

MBEs/WBEs that will perform as subcontractors/suppliers/consultants include the following:

MBE/WBE Firm: **Allpoints Security and Detective, Inc.**

Address: **2112 E. 71st Street, Chicago, IL 60649**

E-mail: **mail@allpointssecurityinc.com**

Contact Person: **Sharon Benson** Phone: **773-955-6700**

Dollar Amount Participation: \$

**12**

%

Percent Amount of Participation:

**X**

No \_\_\_\_\_

\*Letter of Intent attached? Yes **X**

\*Current Letter of Certification attached? Yes **x**

No \_\_\_\_\_

MBE/WBE Firm: \_\_\_\_\_

Address: \_\_\_\_\_

E-mail: \_\_\_\_\_

Contact Person: \_\_\_\_\_ Phone: \_\_\_\_\_

Dollar Amount Participation: \$

Percent Amount of Participation: \_\_\_\_\_ %

\*Letter of Intent attached? Yes \_\_\_\_\_

No \_\_\_\_\_

\*Current Letter of Certification attached? Yes \_\_\_\_\_

No \_\_\_\_\_

*Attach additional sheets as needed.*

\* Letter(s) of Intent and current Letters of Certification must be submitted at the time of bid.

**MBE/WBE LETTER OF INTENT - FORM 2**

M/WBE Firm: Allpoints Security and Detective, Inc.  
Contact Person: **Sharon Benson**  
Address: **2112 E. 71st Street**  
City/State: **Chicago/IL** Zip: **60649**  
Phone: **773-955-6700** Fax: **773-667-9266**  
Email: **mail@allpointssecurityinc.com**

Participation:  Direct  Indirect

Will the M/WBE firm be subcontracting any of the goods or services of this contract to another firm?

No  Yes -- Please attach explanation. Proposed Subcontractor(s): \_\_\_\_\_

The undersigned M/WBE is prepared to provide the following Commodities/Services for the above named Project/ Contract: (If more space is needed to fully describe M/WBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)

Provide equipment repairs, retrievals, collection swap-outs of electronic monitoring equipment.

---

---

---

Indicate the **Dollar Amount, Percentage**, and the **Terms of Payment** for the above-described Commodities/ Services:

The below information is an estimated range that is dependent upon a variety of factors including but not limited to; number of active units, actual number of retrievals per month, etc.

Percentage: 12; Terms of Payment: Monthly

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement for the above work, conditioned upon (1) the Bidder/Proposer's receipt of a signed contract from the County of Cook; (2) Undersigned Subcontractor remaining compliant with all relevant credentials, codes, ordinances and statutes required by Contractor, Cook County, and the State to participate as a MBE/WBE firm for the above work. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/Supply and Fee/Cost were completed.

  
Signature (M/WBE)

Sharon Benson

Print Name

Allpoints Security and Detective, Inc.

Firm Name

May 7, 2018

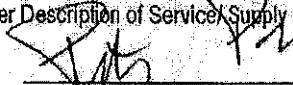
Date

Subscribed and sworn before me

this 7 day of May, 2018

Notary Public



  
Signature (Prime Bidder/Proposer)

Peter Poli

Print Name

Track Group, Inc.

Firm Name

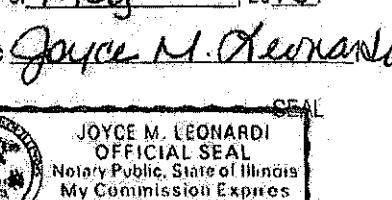
7 May 2018

Date

Subscribed and sworn before me

this 7th day of May, 2018

Notary Public





May 3, 2018

ALEATHA EASLEY, MCA  
Compliance Officer  
Cook County Office of Contract Compliance  
Chicago, IL 60602  
312.603.5504  
[aleatha.easley@cookcountyl.gov](mailto:aleatha.easley@cookcountyl.gov)

Re: MBE/WBE Good Faith Efforts - for RFP 1515-15006

Dear Ms. Easley,

Please consider this letter to represent the documentation and demonstration of Track Group Inc.'s good faith efforts to research certified MBE/WBE firms to determine if other firms (beyond Allpoints Security, LLC whom we have partnered with) were capable of providing participation on this contract. Track Group utilized the below web link to search for certified M/WBE firms to perform the field services (equipment retrieval, inventory management etc.) for this contract.

<https://cookcounty.diversitycompliance.com/>

The services being procured via RFP 1515-15006 for the Cook County Adult Probation Department, the Cook County Juvenile Probation Department, and the Cook County Sheriff's Office are for the secure, electronic monitoring of County offenders/inmates being supervised in the community via secure, ankle-worn tracking and monitoring bracelets. This type of program requires the provision of our proprietary, patented, public safety oriented devices that are not manufactured by anyone else other than Track Group Inc. It also requires the use of our proprietary, custom software interface to monitor and communicate with the devices. Again, no other company/entity can provide the software necessary to utilize these devices. The only service/aspect of this program that can be provided by another entity is the field work described above. Allpoints Security Inc. has been chosen to perform this part of the contract as a subcontractor for Track Group. It requires experience working with criminal offender populations, an office location near the County courts, and experience with electronic monitoring systems. We were unsuccessful in locating another firm who could also perform these duties with the requirements stated herein.

Please let me know if you have any questions or concerns.

Regards,

A handwritten signature in black ink, appearing to read "Matthew Swando".

Matthew Swando  
Vice President of Sales & Marketing  
Track Group Inc.  
[Matthew.swando@trackgrp.com](mailto:Matthew.swando@trackgrp.com)

I.

**POLICY AND GOALS**

- A. It is the policy of the County of Cook to prevent discrimination in the award of or participation in County Contracts and to eliminate arbitrary barriers for participation in such Contracts by local businesses certified as a Minority Business Enterprise (MBE) and Women-owned Business Enterprise (WBE) as both prime and sub-contractors. In furtherance of this policy, the Cook County Board of Commissioners has adopted a Minority- and Women-owned Business Enterprise Ordinance (the "Ordinance") which establishes annual goals for MBE and WBE participation as outlined below:

Contract Type	Goals	
	MBE	WBE
Goods and Services	25%	10%
Construction	24%	10%
Professional Services	35% Overall	

- B. **The County shall set contract-specific goals, based on the availability of MBEs and WBEs that are certified to provide commodities or services specified in this solicitation document. The MBE/WBE participation goals for this Agreement are 25% MBE and 10% WBE.** A Bid, Quotation, or Proposal shall be rejected if the County determines that it fails to comply with this General Condition in any way, including but not limited to: (i) failing to state an enforceable commitment to achieve for this contract the identified MBE/WBE Contract goals; or (ii) failing to include a Petition for Reduction/Waiver, which states that the goals for MBE/WBE participation are not attainable despite the Bidder or Proposer Good Faith Efforts, and explains why. If a Bid, Quotation, or Proposal is rejected, then a new Bid, Quotation, or Proposal may be solicited if the public interest is served thereby.
- C. To the extent that a Bid, Quotation, or Proposal includes a Petition for Reduction/Waiver that is approved by the Office of Contract Compliance, the Contract specific MBE and WBE participation goals may be achieved by the proposed Bidder or Proposer's status as an MBE or WBE; by the Bidder or Proposer's enforceable joint-venture agreement with one or more MBEs and/or WBEs; by the Bidder or Proposer entering into one or more enforceable subcontracting agreements with one or more MBE and WBE; by the Bidder or Proposer establishing and carrying out an enforceable mentor/protégé agreement with one or more MBE and WBE; by the Bidder or Proposer actively engaging the Indirect Participation of one or more MBE and WBE in other aspects of its business; or by any combination of the foregoing, so long as the Utilization Plan evidences a commitment to meet the MBE and WBE Contract goals set forth in (B) above, as approved by the Office of Contract Compliance.
- D. A single Person, as defined in the Procurement Code, may not be utilized as both an MBE and a WBE on the same Contract, whether as a Consultant, Subcontractor or supplier.
- E. Unless specifically waived in the Bid or Proposal Documents, this Exhibit; the Ordinance; and the policies and procedures promulgated thereunder shall govern. If there is a conflict

between this Exhibit and the Ordinance or the policies and procedures, the Ordinance shall control.

- F. A Consultant's failure to carry out its commitment regarding MBE and WBE participation in the course of the Contract's performance may constitute a material breach of the Contract. If such breach is not appropriately cured, it may result in withholding of payments under the Contract, contractual penalties, disqualification and any other remedy provided for in Division 4 of the Procurement Code at law or in equity.

## **II. REQUIRED BID OR PROPOSAL SUBMITTALS**

A Bidder or Proposer shall document its commitment to meeting the Contract specific MBE and WBE participation goals by submitting a Utilization Plan with the Bid or Proposal. The Utilization Plan shall include (1) one or more Letter(s) of Intent from the relevant MBE and WBE firms; and (2) current Letters of Certification as an MBE or WBE. Alternatively, the Bidder or Proposer shall submit (1) a written Petition for Reduction/Waiver with the Bid, Quotation or Proposal, which documents its preceding Good Faith Efforts and an explanation of its inability to meet the goals for MBE and WBE participation. The Utilization Plan shall be submitted at the time that the bid or proposal is due. **Failure to include a Utilization Plan will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

### **A. MBE/WBE Utilization Plan**

Each Bid or Proposal shall include a complete Utilization Plan, as set forth on Form 1 of the M/WBE Compliance Forms. The Utilization Plan shall include the name(s), mailing address, email address, and telephone number of the principal contact person of the relevant MBE and WBE firms. If the Bidder or Proposer submits a Bid or Proposal, and any of their subconsultants, suppliers or consultants, are certified MBE or WBE firms, they shall be identified as an MBE or WBE within the Utilization Plan.

#### **1. Letter(s) of Intent**

Except as set forth below, a Bid or Proposal shall include, as part of the Utilization Plan, one or more Letter(s) of Intent, as set forth on Form 2 of the M/WBE Compliance Forms, executed by each MBE and WBE and the Bidder or Proposer. The Letter(s) of Intent will be used to confirm that each MBE and WBE shall perform work as a Subcontractor, supplier, joint venture, or consultant on the Contract. Each Letter of Intent shall indicate whether and the degree to which the MBE or WBE will provide goods or services directly or indirectly during the term of the Contract. The box for direct participation shall be marked if the proposed MBE or WBE will provide goods or services directly related to the scope of the Contract. The box for Indirect participation shall be marked if the proposed MBE or WBE will not be directly involved in the Contract but will be utilized by the Bidder or Proposer for other services not related to the Contract. Indirect Participation shall not be counted toward the participation goal. Each Letter of Intent shall accurately detail the work to be performed by the relevant MBE or WBE firm, the agreed dollar amount, the percentage of work, and the terms of payment.

**Failure to include Letter(s) of Intent will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

All Bids and Proposals must conform to the commitments made in the corresponding Letter(s) of Intent, as may be amended through change orders.

The Contract Compliance Director may at any time request supplemental information regarding Letter(s) of Intent, and such information shall be furnished if the corresponding Bid or Proposal is to be deemed responsive.

**2. Letter(s) of Certification**

Only current Letter(s) of Certification from one of the following entities may be accepted as proof of certification for MBE/WBE status, provided that Cook County's requirements for certification are met:

- County of Cook
- City of Chicago

Persons that are currently certified by the City of Chicago in any area other than Construction/Public Works shall also complete and submit a MBE/WBE Reciprocal Certification Affidavit along with a current letter of certification from the City of Chicago. This Affidavit form can be downloaded from [www.cookcountyil.gov/contractcompliance](http://www.cookcountyil.gov/contractcompliance).

The Contract Compliance Director may reject the certification of any MBE or WBE on the ground that it does not meet the requirements of the Ordinance, or the policies and rules promulgated thereunder.

**3. Joint Venture Affidavit**

In the event a Bid or Proposal achieves MBE and/or WBE participation through a Joint Venture, the Bid or Proposal shall include the required Joint Venture Affidavit, which can be downloaded from [www.cookcountyil.gov/contractcompliance](http://www.cookcountyil.gov/contractcompliance). The Joint Venture Affidavit shall be submitted with the Bid or Proposal, along with current Letter(s) of Certification.

**B. Petition for Reduction/Waiver**

In the event a Bid or Proposal does not meet the Contract specific goals for MBE and WBE participation, the Bid or Proposal shall include a Petition for Reduction/Waiver, as set forth on Form 3. The Petition for Reduction/Waiver shall be supported by sufficient evidence and documentation to demonstrate the Bidder or Proposer's Good Faith Efforts in attempting to achieve the applicable MBE and WBE goals, and its inability to do so despite its Good Faith Efforts.

**Failure to include Petition for Reduction/Waiver will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

### **III. REDUCTION/WAIVER OF MBE/WBE GOALS**

#### **A. Granting or Denying a Reduction/Waiver Request.**

1. The adequacy of the Good Faith Efforts to utilize MBE and WBE firms in a Bid or Proposal will be evaluated by the CCD under such conditions as are set forth in the Ordinance, the policies and rules promulgated thereunder, and in the "Petition for Reduction/Waiver of MBE/WBE Participation Goals" – Form 3 of the M/WBE Compliance Forms.
2. With respect to a Petition for Reduction/Waiver, the sufficiency or insufficiency of a Bidder or Proposer's Good Faith Efforts shall be evaluated by the CCD as of the date upon which the corresponding Bid or Proposal was due.
3. The Contract Compliance Director or his or her duly authorized Waiver Committee may grant or deny the Petition for Reduction/Waiver based upon factors including but not limited to: (a) whether sufficient qualified MBE and WBE firms are unavailable despite good faith efforts on the part of the Bidder or Proposer; (b) the degree to which specifications and the reasonable and necessary requirements for performing the Contract make it impossible or economically infeasible to divide the Contract into sufficiently small tasks or quantities so as to enable the Bidder or Proposer to utilize MBE and WBE firms in accordance with the applicable goals; (c) the degree to which the prices or prices required by any potential MBE or WBE are more than 10% above competitive levels; and (d) such other factors as are determined relevant by the Contract Compliance Director or the duly authorized Waiver Committee.
4. If the Contract Compliance Director or the duly authorized Waiver Committee determines that the Bidder or Proposer has not demonstrated sufficient Good Faith Efforts to meet the applicable MBE and WBE goals, the Contract Compliance Director or the duly authorized Waiver Committee may deny a Petition for Reduction/Waiver, declare the Bid or Proposal non-responsive, and recommend rejection of the Bid, Quotation, or Proposal.

### **IV. CHANGES IN CONSULTANT'S UTILIZATION PLAN**

- A. A Consultant, during its performance of the Contract, may not change the original MBE or WBE commitments specified in the relevant Utilization Plan, including but not limited to, terminating a MBE or WBE Contract, reducing the scope of the work to be performed by a MBE/WBE, or decreasing the price to a MBE/WBE, except as otherwise provided by the Ordinance and according to the policies and procedures promulgated thereunder.

- B. Where a Person listed under the Contract was previously considered to be a MBE or WBE but is later found not to be, or work is found not to be creditable toward the MBE or WBE goals as stated in the Utilization Plan, the Consultant shall seek to discharge the disqualified enterprise, upon proper written notification to the Contract Compliance Director, and make every effort to identify and engage a qualified MBE or WBE as its replacement. Failure to obtain an MBE or WBE replacement within 30 business days of the Contract Compliance Director's written approval of the removal of a purported MBE or WBE may result in the termination of the Contract or the imposition of such remedy authorized by the Ordinance, unless a written Petition for Reduction/Waiver is granted allowing the Consultant to award the work to a Person that is not certified as an MBE or WBE.

#### **V. NON-COMPLIANCE**

If the CCD determines that the Consultant has failed to comply with its contractual commitments or any portion of the Ordinance, the policies and procedures promulgated thereunder, or this Exhibit, the Contract Compliance Director shall notify the Consultant of such determination and may take any and all appropriate actions as set forth in the Ordinance or the policies and procedures promulgated thereunder which includes but is not limited to disqualification, penalties, withholding of payments or other remedies in law or equity.

#### **VI. REPORTING/RECORD-KEEPING REQUIREMENTS**

The Consultant shall comply with the reporting and record-keeping requirements in the manner and time established by the Ordinance, the policies and procedure promulgated thereunder, and the Contract Compliance Director. Failure to comply with such reporting and record-keeping requirements may result in a declaration of Contract default. Upon award of a Contract, a Consultant shall acquire and utilize all Cook County reporting and record-keeping forms and methods which are made available by the Office of Contract Compliance. MBE and WBE firms shall be required to verify payments made by and received from the prime Consultant.

#### **VII. EQUAL EMPLOYMENT OPPORTUNITY**

Compliance with MBE and WBE requirements will not diminish or supplant other legal Equal Employment Opportunity and Civil Rights requirements that relate to Consultant and Subcontractor obligations.

Any questions regarding this section should be directed to:

Contract Compliance Director

Cook County

118 North Clark Street, Room 1020

Chicago, Illinois 60602

(312) 603-5502

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 4

Evidence of Insurance



# CERTIFICATE OF LIABILITY INSURANCE

358118

DATE (MM/DD/YYYY)  
4/4/2018

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERNS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. IF SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER		CONTACT NAME: Dianna Sarabia
USI Insurance Services National, Inc. 10 S. Wacker, 17th floor Chicago, IL 60606		PHONE (A/C, No. Ext): 312.766.2038
		FAX (A/C, No):
		E-MAIL: dianna.sarabia@usi.com
		INSURER(S) AFFORDING COVERAGE
		NAIC #
INSURER A: Lloyd's of London		
INSURER B: Valley Forge Insurance Company		20508
INSURER C: Travelers Property Casualty Co of America		25674
INSURER D: American Casualty Company of Reading, PA		20427
INSURER E: Transportation Insurance Company		20494
INSURER F:		

## COVERAGES

CERTIFICATE NUMBER: 12931175

REVISION NUMBER: See below

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS		
A	X COMMERCIAL GENERAL LIABILITY  CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR	X	X	CJ10028218  Occurrence \$25K Ded  EBL retro date 8/1/2015	3/31/2018	3/31/2019	EACH OCCURRENCE	\$ 1,000,000	
							DAMAGE TO RENTED PREMISES (Ex occurrence)	\$ 100,000	
							MED EXP (Any one person)	\$ 1,000	
							PERSONAL & ADV INJURY	\$ 3,000,000	
							GENERAL AGGREGATE	\$ 3,000,000	
							PRODUCTS - COMP/OP AGG	\$ 3,000,000	
							Employee Benefits	\$ 1,000,000	
B	AUTOMOBILE LIABILITY  X ANY AUTO OWNED AUTOS ONLY Hired AUTOS ONLY <input checked="" type="checkbox"/> SCHEDULED AUTOS NON-OWNED AUTOS ONLY			6057537710	3/31/2018	3/31/2019	COMBINED SINGLE LIMIT (Ex accident)	\$ 1,000,000	
							BODILY INJURY (Per person)	\$	
							BODILY INJURY (Per accident)	\$	
							PROPERTY DAMAGE (Per accident)	\$	
C	UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE			ZUP-31M95068-18-NF	3/31/2018	3/31/2019	EACH OCCURRENCE	\$ 1,000,000	
							AGGREGATE	\$ 1,000,000	
								\$	
D	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y / N <input type="checkbox"/> N	N / A X	6057043119	3/31/2018	3/31/2019	X PER STATUTE	OTH-ER	
							E.L. EACH ACCIDENT	\$ 1,000,000	
							E.L. DISEASE - EA EMPLOYEE	\$ 1,000,000	
							E.L. DISEASE - POLICY LIMIT	\$ 1,000,000	
A	Professional Liability/E&O			CJ10028218 Claims Made \$25K Ded Retro Date: 01/30/2003	3/31/18	3/31/19	General Aggregate: \$3,000,000		

## DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Evidence of Insurance includes:

Lloyds of London Policy# CJ10028218

-Sexual Misconduct Liability Limit \$1,000,000

Certificate holder is named as an additional insured as it relates to general liability &amp; waiver of subrogation is granted as it relates to the general liability in accordance with the terms and conditions of the policies. Umbrella follows form as it relates to additional insureds.

## CERTIFICATE HOLDER

## CANCELLATION

Cook County Chief Procurement Officer 118 North Clark St. Room 1018 Chicago, IL 60602	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE  <i>Jean Branda</i>

The ACORD name and logo are registered marks of ACORD © 1988-2015 ACORD CORPORATION. All rights reserved.

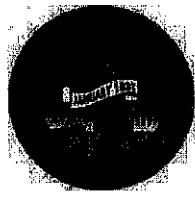
**Certificate of Insurance (Con't)****OTHER Coverage**

INSR LTR	TYPE OF INSURANCE INSR	ADDL INSR	WVD SUBR	POLICY NUMBER	EFFECTIVE DATE (MM/DD/YY)	EXPIRATION DATE (MM/DD/YY)	LIMIT
E	Workers Compensation-CA			6057043122	3/31/2018	3/31/2019	\$1,000,000

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 5

Board Authorization



# Board of Commissioners of Cook County

118 North Clark Street  
Chicago, IL

## Legislation Details (With Text)

<b>File #:</b>	19-1293	<b>Version:</b>	1	<b>Name:</b>	Track Group, Inc., Naperville, Illinois
<b>Type:</b>	Contract			<b>Status:</b>	Approved
<b>File created:</b>	1/15/2019			<b>In control:</b>	Board of Commissioners
<b>On agenda:</b>	1/24/2019			<b>Final action:</b>	1/24/2019
<b>Title:</b>	PROPOSED CONTRACT				

**Department(s):** Adult and Juvenile Probation Departments; Circuit Court of Cook County; Cook County Sheriff's Department

**Vendor:** Track Group, Inc., Naperville, Illinois

**Request:** Authorization for the Chief Procurement Officer to enter into and execute

**Good(s) or Service(s):** Electronic Monitoring Services - Global Positioning System (GPS)

**Contract Value:** \$4,064,311.50

**Contract period:** 1/28/2019 - 1/27/2022, with two (2), one (1) year renewal options

**Potential Fiscal Year Budget Impact:**

Adult Probation Department

FY 2019 \$680,725.00, FY 2020 \$816,870.00, FY 2021 \$816,870.00 and FY 2022 \$136,145.00;

Juvenile Probation Department

FY 2019 \$310,684.00, FY 2020 \$369,380.00, FY 2021 \$369,380.00 and FY 2022 \$58,696.00;

Sheriff's Department

FY 2019 \$140,430.00, FY 2020 \$168,516.00, FY 2021 \$168,516.00 and FY 2022 \$28,099.50

**Accounts:** (Adult Probation 1280-540131, Maintenance and Subscription Services); (Juvenile Probation 1326-540130, Maintenance and Subscription Services); (Sheriff's Department 1239-540130)

**Contract Number(s):** 1515-15006B

**Concurrences:**

The vendor has met the Minority- and Women-owned Business Enterprise Ordinance via direct participation and full MBE and partial WBE waiver.

The Chief Procurement Officer concurs.

**Summary:** Track Group, Inc. will provide electronic monitoring and Global Positioning System (GPS) services for the Adult Probation Department, the Juvenile Probation and Court Services Department and the Cook County Sheriff's Office for youth and adults who are ordered by the court to wear electronic monitoring devices.

Track Group, Inc. will provide GPS monitoring equipment and services for adult probationers and pretrial defendants in order to comply with Public Act 95-0773, also known as the Cindy Bischof Law, which calls for the monitoring of certain domestic violence offenses to be monitored by the Adult Probation Department Home Confinement Unit as a condition of bail or probation. Offenders are ordered to wear a GPS tracking device to help monitor compliance with orders to stay away from the complaining witness, the complaining witness's home/workplace, or any other protected address specified. There are currently more than 350 adults under GPS monitoring and 110 victims who carry

GPS devices to create mobile exclusion zones. Effective January 1, 2015, new legislation (Public Act 98-1012, 725 ILCS 5/110-5) significantly expanded the types of charges required to be considered for GPS monitoring as a condition of bail.

GPS technology is used by the Juvenile Probation and Court Services Department to monitor high-risk minors in home confinement as an alternative to secure detention or as condition of release into the community. These devices are deployed at various points of the judicial process from pre-adjudication through post-dispositional stages of court proceedings.

The contract was awarded through the Request for Proposals (RFP) process in accordance with the Cook County Procurement Code. Track Group, Inc. was selected based on established evaluation criteria.

**Sponsors:**

**Indexes:** TIMOTHY C. EVANS, Chief Judge, Circuit Court of Cook County.

**Code sections:**

**Attachments:**

Date	Ver.	Action By	Action	Result
1/24/2019	1	Board of Commissioners		

**PROPOSED CONTRACT**

**Department(s):** Adult and Juvenile Probation Departments, Circuit Court of Cook County; Cook County Sheriff's Department

**Vendor:** Track Group, Inc., Naperville, Illinois

**Request:** Authorization for the Chief Procurement Officer to enter into and execute

**Good(s) or Service(s):** Electronic Monitoring Services - Global Positioning System (GPS)

**Contract Value:** \$4,064,311.50

**Contract period:** 1/28/2019 - 1/27/2022, with two (2), one (1) year renewal options

**Potential Fiscal Year Budget Impact:**

Adult Probation Department

FY 2019 \$680,725.00, FY 2020 \$816,870.00, FY 2021 \$816,870.00 and FY 2022 \$136,145.00;

Juvenile Probation Department

FY 2019 \$310,684.00, FY 2020 \$369,380.00, FY 2021 \$369,380.00 and FY 2022 \$58,696.00;

Sheriff's Department

FY 2019 \$140,430.00, FY 2020 \$168,516.00, FY 2021 \$168,516.00 and FY 2022 \$28,099.50

**Accounts:** (Adult Probation 1280-540131, Maintenance and Subscription Services); (Juvenile Probation 1326-540130, Maintenance and Subscription Services); (Sheriff's Department 1239-540130)

**Contract Number(s):** 1515-15006B

**Concurrences:**

The vendor has met the Minority- and Women-owned Business Enterprise Ordinance via direct participation and full MBE and partial WBE waiver.

The Chief Procurement Officer concurs.

**Summary:** Track Group, Inc. will provide electronic monitoring and Global Positioning System (GPS) services for the Adult Probation Department, the Juvenile Probation and Court Services Department and the Cook County Sheriff's Office for youth and adults who are ordered by the court to wear electronic monitoring devices.

Track Group, Inc. will provide GPS monitoring equipment and services for adult probationers and pretrial defendants in order to comply with Public Act 95-0773, also known as the Cindy Bischof Law, which calls for the monitoring of certain domestic violence offenses to be monitored by the Adult Probation Department Home Confinement Unit as a condition of bail or probation. Offenders are ordered to wear a GPS tracking device to help monitor compliance with orders to stay away from the complaining witness, the complaining witness's home/workplace, or any other protected address specified. There are currently more than 350 adults under GPS monitoring and 110 victims who carry GPS devices to create mobile exclusion zones. Effective January 1, 2015, new legislation (Public Act 98-1012, 725 ILCS 5/110-5) significantly expanded the types of charges required to be considered for GPS monitoring as a condition of bail.

GPS technology is used by the Juvenile Probation and Court Services Department to monitor high-risk minors in home confinement as an alternative to secure detention or as condition of release into the community. These devices are deployed at various points of the judicial process from pre-adjudication through post-dispositional stages of court proceedings.

The contract was awarded through the Request for Proposals (RFP) process in accordance with the Cook County Procurement Code. Track Group, Inc. was selected based on established evaluation criteria.

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 6

CJIS Security Policy

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the  
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
  - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
  - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
  - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION**  
**CRIMINAL JUSTICE INFORMATION SERVICES**  
**SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

**1.00 Definitions**

**1.01 Contracting Government Agency (CGA)** - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

**1.02 Contractor** - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

**2.00 Responsibilities of the Contracting Government Agency.**

**2.01** The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

**3.00 Responsibilities of the Contractor.**

**3.01** The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

**4.00 Security Violations.**

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM

**CERTIFICATION**

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Matt Edwards

Printed Name/Signature of Contractor Employee

18 January 2019

Date

PETER POLI

Printed Name/Signature of Contractor Representative

18 January 2019

Date

TRACK GROUP, INC. - Chief Financial Officer

Organization and Title of Contractor Representative

## **APPENDIX I REFERENCES**

---

- White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008
- [CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306
- [FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306
- [FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III—Information Security
- [FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004
- [FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006
- [FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1
- [NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14
- [NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25
- [NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–30
- [NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32
- [NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34
- [NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35
- [NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36
- [NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39
- [NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40
- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

- [NIST SP 800-45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800-45, Version 2
- [NIST SP 800-46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800-46
- [NIST SP 800-48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800-48
- [NIST SP 800-52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800-52
- [NIST SP 800-53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800-53, Revision 2
- [NIST SP 800-53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800-53A
- [NIST SP 800-58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800-58
- [NIST SP 800-60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800-60, Revision 1, DRAFT
- [NIST SP 800-63-1] *Electronic Authentication Guideline*; NIST Special Publication 800-63-1; DRAFT
- [NIST SP 800-64] NIST Special Publication 800-64
- [NIST SP 800-66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800-66
- [NIST SP 800-68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800-68
- [NIST SP 800-70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800-70
- [NIST SP 800-72] *Guidelines on PDA Forensics*; NIST Special Publication 800-72
- [NIST SP 800-73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800-73; Revision 1
- [NIST SP 800-76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800-76
- [NIST SP 800-77] *Guide to IPsec VPNs*; NIST Special Publication 800-77
- [NIST SP 800-78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800-78
- [NIST SP 800-81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800-81
- [NIST SP 800-84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800-84

- [NIST SP 800-86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800-86
- [NIST SP 800-87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800-87
- [NIST SP 800-96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800-96
- [NIST SP 800-97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800-97
- [NIST SP 800-121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800-124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800-145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800-146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A-130] *Management of Federal Information Resources*; Circular No. A-130; Revised; February 8, 1996
- [OMB M-04-04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04-04; December 16, 2003
- [OMB M-06-15] *Safeguarding Personally Identifiable Information*; OMB Memo 06-15; May 22, 2006
- [OMB M-06-16] *Protection of Sensitive Agency Information*; OMB Memo 06-16; June 23, 2006
- [OMB M-06-19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06-19; July 12, 2006
- [OMB M-07-16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07-16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings
- [USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

## **APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE**

---

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
  - a. 3.2.9 – Local Agency Security Officer (LASO)
  - b. 5.1.1.6 – Agency User Agreements
  - c. 5.1.1.7 – Outsourcing Standards for Channelers\*
  - d. 5.1.3 – Secondary Dissemination
  - e. 5.2.1.1 – All Personnel (Security Awareness Training)
  - f. 5.3 – Incident Response
  - g. 5.4 – Auditing and Accountability
  - h. 5.8 – Media Protection
  - i. 5.9.2 – Controlled Area
  - j. 5.11 – Formal Audits \*\*
  - k. 5.12 – Personnel Security\*\*\*

\* Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

\*\*Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

\*\*\* Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
  - a. 5.5.2.4 – Access Control – Encryption
  - b. 5.6 – Identification and Authentication (web-site access)
  - c. 5.10.1.2 – System and Communications Protection – Encryption
4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
  - a. 5.5.2.4 – Access Control – Encryption
  - b. 5.6 – Identification and Authentication
  - c. 5.7 – Configuration Management
  - d. 5.10 – System and Communications Protection and Information Integrity
5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
  - a. 5.7 – Configuration Management
  - b. 5.10 – System and Communications Protection and Information Integrity
6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

## **APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE**

---

This supplemental guidance is directed toward those criminal justice agencies that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and, may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as “terminal agencies”. The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:

- a. 3.2.9 – Local Agency Security Officer (LASO)
- b. 5.1.1.3 – Criminal Justice Agency User Agreements
- c. 5.1.3 – Secondary Dissemination
- d. 5.2.1.1 – Security Awareness Training
- e. 5.3 – Incident Response
- f. 5.4.6 – Audit Record Retention
- g. 5.8 – Media Protection
- h. 5.9 – Physical Security
- i. 5.10.2 – Facsimile Transmission of CJI
- j. 5.11 – Formal Audits\*
- k. 5.12 – Personnel Security

\*Note: States shall triennially audit all CJAs

2. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:

- a. 5.5.2.4 – Access Control – Encryption
- b. 5.6 – Identification and Authentication
- c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
  - a. 5.5.2.4 – Access Control – Encryption
  - b. 5.6 – Identification and Authentication
  - c. 5.7 – Configuration Management
  - d. 5.10 – System and Communications Protection and Information Integrity

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 7

Cook County Information Technology Special Conditions (ITSC)

**Exhibit 7**  
**Cook County Information Technology Special Conditions (ITSCs)**

**1. DEFINITIONS FOR SPECIAL CONDITIONS**

1.1.     **"Assets"** means Equipment, Software, Intellectual Property, IP Materials and other assets used in providing the Services. Assets are considered in use as of the date of deployment.

1.2.     **"Business Associate Agreement"** or **"BAA"** means an agreement that meets the requirements of 45 C.F.R. 164.504(e).

1.3.     **"Business Continuity Plan"** means the planned process, and related activities, required to maintain continuity of business operations between the period of time following declaration of a Disaster until such time an IT environment is returned to an acceptable condition of normal business operation.

1.4.     **"Cardholder Data"** means data that meets the definition of "Cardholder Data" in the most recent versions of the Payment Card Industry's Data Security Standard.

1.5.     **"Change"** means, in an operational context, an addition, modification or deletion to any Equipment, Software, IT environment, IT systems, network, device, infrastructure, circuit, documentation or other items related to Services. Changes may arise reactively in response to Incidents/Problems or externally imposed requirements (e.g., legislative changes), or proactively from attempts to (a) seek greater efficiency or effectiveness in the provision or delivery of Services; (b) reflect business initiatives; or (c) implement programs, projects or Service improvement initiatives.

1.6.     **"Change Management"** means, in an operational context, the Using Agency approved processes and procedures necessary to manage Changes with the goal of enabling Using Agency-approved Changes with minimum disruption.

1.7.     **"Change Order"** means a document that authorizes a Change to the Services or Deliverables under the Agreement, whether in time frames, costs, or scope.

1.8.     **"Change Request"** means one Party's request to the other Party for a Change Order.

1.9.     **"Contractor"** has the same meaning as either: (a) both "Contractor" and "Consultant" as such terms are defined, and may be interchangeably used in the County's Professional Services Agreement, if such document forms the basis of this Agreement or (b) "Contractor" as defined in the County's Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.10.    **"Contractor Confidential Information"** means all non-public proprietary information of Contractor that is marked confidential, restricted, proprietary, or with a similar designation; provided that Contractor Confidential Information excludes: (a) Using Agency Confidential Information, (b) Using Agency Data; (c) information that may be subject to disclosure under Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances; and (d) the terms of this Agreement, regardless of whether marked with a confidential designation or not.

1.11.    **"Contractor Facilities"** means locations owned, leased or otherwise utilized by

Contractor and its Subcontractors from which it or they may provide Services.

1.12. "**Contractor Intellectual Property**" means all Intellectual Property owned or licensed by Contractor.

1.13. "**Contractor IP Materials**" means all IP Materials owned or licensed by Contractor.

1.14. "**Contractor Personnel**" means any individuals that are employees, representatives, Subcontractors or agents of Contractor, or of a direct or indirect Subcontractor of Contractor.

1.15. "**Contractor-Provided Equipment**" means Equipment provided by or on behalf of Contractor."

1.16. "**Contractor-Provided Software**" means Software provided by or on behalf of Contractor.

1.17. "**Criminal Justice Information**" means data that meets the definition of "Criminal Justice Information" in the most recent version of FBI's CJIS Security Policy and also data that meets the definition of "Criminal History Record Information" at 28 C.F.R. 20.

1.18. "**Critical Milestone**" means those milestones critical to the completion of the Services as identified in this Agreement, in any work plan, project plan, statement of work, or other document approved in advance by the Using Agency.

1.19. "**Data Protection Laws**" means laws, regulations, regulatory requirements, industry self-regulatory standards, and codes of practice in connection with the processing of Personal Information, including those provisions of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §§ 1320(d) et seq.) as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. §§ 17921 et seq.) and the Payment Card Industry standards.

1.20. "**Data Security Breach**" means (a) the loss or misuse (by any means) of any Using Agency Data or other Using Agency Confidential Information; (b) the unauthorized or unlawful access, use, or disclosure of any Using Agency Data or other Using Agency Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity or availability of any Using Agency Data or other Using Agency Confidential Information.

1.21. "**Deliverable**" has the same meaning as either: (a) "Deliverable" as defined in the County's Professional Services Agreement, if such document forms the basis of this Agreement; or (b) "Deliverable" as defined in the County's Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement. In either case, Deliverables includes without limitation Contractor-Provided Equipment, Contractor-Provided Software, Developed Intellectual Property.

1.22. "**Developed Intellectual Property**" means Intellectual Property as well as any IP Materials conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services, including, but not limited to: (a) modifications to, or enhancements (derivative works) of, the Using Agency Intellectual Property or the Using Agency IP Materials; (b) Developed Software; (c) documentation, training materials, or other IP Materials that do not modify or enhance then existing Using Agency IP Materials; and (d) modifications to or enhancements (derivative works) of, Third Party Intellectual Property or related IP Materials to the extent not owned by the licensor of the Third Party Intellectual Property under the terms of the applicable license.

1.23. "**Developed Software**" any Software conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services (including any modifications, enhancements, patches, upgrades or similar developments).

1.24. "**Disaster**" means a sudden, unplanned, calamitous event causing substantial damage or loss as defined or determined by a risk assessment and business impact analysis, and which creates an inability or substantial impairment on the organization's part to provide critical business functions for a material period of time. This also includes any period when the Using Agency management decides to divert resources from normal production responses and exercises its Disaster Recovery Plan.

1.25. "**Disaster Recovery Plan**" means the planned process, and related activities, required to return an IT environment to an acceptable condition of normal business operation following declaration of a Disaster.

1.26. "**Equipment**" means the computer, telecommunications, network, storage, and related hardware and peripherals owned or leased by the Using Agency or its Third Party Contractors, or by Contractor or its Subcontractors, and used or supported by Contractor or its Subcontractors, or by the Using Agency or its agents, in connection with the Services.

1.27. "**Exit Assistance Plan**" means a detailed plan for the delivery of the Exit Assistance Services.

1.28. "**Exit Assistance Period**" has the meaning given in Section 9.2.

1.29. "**Exit Assistance Services**" means such exit assistance services as are reasonably necessary from Contractor and/or its Subcontractors to enable a complete transition of the affected Services to the Using Agency or the Using Agency's designee(s), including, but not limited to, all of the services, tasks and functions described in Section 9.

1.30. "**Illicit Code**" means any hidden files, automatically replicating, transmitting or activating computer program, virus (or other harmful or malicious computer program) or any Equipment-limiting, Software-limiting or Services-limiting function (including, but not limited to, any key, node lock, time-out or similar function), whether implemented by electronic or other means.

1.31. "**Incident**" means any event that is not part of the standard operation of a service in the Using Agency IT environment (including an event in respect of the Services or any Equipment or Software) and that causes, or may cause, an interruption to, or a reduction in the quality of, that service. The Using Agency will determine the severity level of each reported Incident.

1.32. "**Intellectual Property**" means any inventions, discoveries, designs, processes, software, documentation, reports, and works of authorship, drawings, specifications, formulae, databases, algorithms, models, methods, techniques, technical data, discoveries, know how, trade secrets, and other technical proprietary information and all patents, copyrights, mask works, trademarks, service marks, trade names, service names, industrial designs, brand names, brand marks, trade dress rights, Internet domain name registrations, Internet web sites and corporate names, and applications for the registration or recordation of any of the foregoing.

1.33. "**IP Materials**" means works of authorship, software, documentation, processes, designs, drawings, specifications, formulae, databases, algorithms, models, methods, processes and techniques,

technical data, inventions, discoveries, know how, the general format, organization, or structure of any report, document or database, and other technical proprietary information.

1.34. **"Laws"** means all United States federal, state and local laws or foreign laws, constitutions, statutes, codes, rules, regulations, ordinances, executive orders, decrees, edicts of or by any governmental authority having the force of law or any other legal requirement (including common law), including Data Protection Laws and the Cook County Code of Ordinances.

1.35. **"Open Source Materials"** means any Software that: (a) contains, or is derived in any manner (in whole or in part) from, any Software that is distributed as free Software, open source Software, shareware (e.g., Linux), or similar licensing or distribution models; and (b) is subject to any agreement with terms requiring that such Software be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributable. Open Source Materials includes without limitation "open source" code (as defined by the Open Source Initiative) and "free" code (as defined by the Free Software Foundation).

1.36. **"Party"** means either County, on behalf of County and its Using Agencies, or Contractor.

1.37. **"Parties"** means both County, on behalf of County and its Using Agencies, and Contractor.

1.38. **"Personal Information"** means personal data or information that relates to a specific, identifiable, individual person, including Using Agency personnel and individuals about whom the Using Agency, Contractor, Contractor's Subcontractors or affiliates has or collects financial and other information. For the avoidance of doubt, Personal Information includes the following: (a) any government-issued identification numbers (e.g., Social Security, driver's license, passport); (b) any financial account information, including account numbers, credit card numbers, debit card numbers, and other Cardholder Data; (c) Criminal Justice Information; (d) Protected Health Information; (e) user name or email address, in combination with a password or security question and answer that would permit access to an account; and (f) any other personal data defined as personally identifiable information under the breach notification laws of the fifty states.

1.39. **"Problem"** means the underlying cause of one or more Incidents, including where such cause is unknown or where it is known and a temporary work-around or permanent alternative has been identified.

1.40. **"Protected Health Information"** or PHI shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. 160.103.

1.41. **"Public Record"** shall have the same meaning as the term "public record" in the Illinois Local Records Act, 50 ILCS 205/1 et seq.

1.42. **"Required Consent"** means that consent required to secure any rights of use of or access to any of Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency Intellectual Property, Using Agency IP Materials, any other Equipment, any other Software whether Third Party Software or otherwise, any other Intellectual Property whether Third Party Intellectual Property or otherwise, any other IP Material, any of which are required by, requested by, used by or accessed by Contractor, its Subcontractors, employees or other agents in connection with the Services.

1.43. “**Services**” either: (a) has the same meaning as “Services” as defined in Article 3 of the County’s Professional Services Agreement, if such document forms the basis of this Agreement or (b) collectively means all of Contractor’s services and other acts required in preparing, developing, and tendering the Using Agency’s Deliverables as “Deliverables” is defined in the County’s Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.44. “**Service Level Agreements**” or “**SLA**” means service level requirement and is a standard for performance of Services, which sets Contractor and Using Agency expectations, and specifies the metrics by which the effectiveness of service activities, functions and processes will be measured, examined, changed and controlled.

1.45. “**Software**” means computer software, including source code, object, executable or binary code, comments, screens, user interfaces, data structures, data libraries, definition libraries, templates, menus, buttons and icons, and all files, data, materials, manuals, design notes and other items and documentation related thereto or associated therewith.

1.46. “**Third Party**” means a legal entity, company or person that is not a Party to the Agreement and is not a Using Agency, Subcontractor, affiliate of a Party, or other entity, company or person controlled by a Party.

1.47. “**Third Party Intellectual Property**” means all Intellectual Property owned by a Third Party, including Third Party Software.

1.48. “**Third Party Contractor**” means a Third Party that provides the Using Agency with products or services that are related to, or in support of, the Services. Subcontractors of Contractor are not “Third Party Contractors.”

1.49. “**Third Party Software**” means a commercial Software product developed by a Third Party not specifically for or on behalf of the Using Agency. For clarity, custom or proprietary Software, including customizations to Third Party Software, developed by or on behalf of the Using Agency to the Using Agency’s specifications shall not be considered Third Party Software.

1.50. “**Using Agency**” has the same meaning as the term “Using Agency” in the Cook County Procurement Code, located at Chapter 34, Article IV in the Cook County Code of Ordinances as amended, as applied to each department or agency receiving goods, Services or other Deliverables under this Agreement and includes Cook County, a body politic and corporate of the State of Illinois, on behalf of such Using Agency.

1.51. “**Using Agency Confidential Information**” means: (a) all non-public proprietary information of Using Agency that is marked confidential, restricted, proprietary, or with a similar designation; (b) Using Agency Data; and (c) any information that is exempt from public disclosure under the Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances.

1.52. “**Using Agency Data**” means all data, whether Personal Information or other data, provided by the Using Agency to Contractor, provided by Third Parties to Contractor for purposes relating to this Agreement, or otherwise encountered by Contractor for purposes relating to this Agreement, including all data sent to Contractor by the Using Agency and/or stored by Contractor on any media relating to the Agreement, including metadata about such data. To the extent there is any uncertainty as to whether any data constitutes Using Agency Data, the data in question shall be treated as Using Agency

Data. Using Agency Data further includes information that is: (a) input, processed or stored by the Using Agency's IT systems, including any Using Agency-Provided Software; (b) submitted to Contractor or its Subcontractors by any employees, agents, the Using Agency, Third Parties, business partners, and customers in connection with the Services or otherwise; (c) Incident records containing information relating to the Services; (d) Using Agency Intellectual Property and Using Agency IP Materials; (e) any raw data used to generate reports under this Agreement and any data included therein; and (f) Using Agency Confidential Information.

1.53. "***Using Agency Intellectual Property***" means all Intellectual Property owned or licensed by the Using Agency, including Developed Intellectual Property.

1.54. "***Using Agency IP Materials***" means all IP Materials owned or licensed by the Using Agency.

1.55. "***Using Agency-Provided Equipment***" means Equipment provided by or on behalf of Using Agency.

1.56. "***Using Agency-Provided Software***" means Software provided by or on behalf of Using Agency.

1.57. "***WISP***" means written information security program.

## **2. SERVICES AND DELIVERABLES**

2.1. Approved Facilities. Contractor will perform Services only within the continental United States and only from locations owned, leased or otherwise utilized by Contractor and its Subcontractors.

2.2. Licenses and Export Controls. Contractor will be responsible for obtaining all necessary export authorizations and licenses for export of technical information or data relating to Using Agency Data, Software, Intellectual Property, IP Materials, or otherwise under this Agreement.

2.3. Required Consents for Assets in Use and Third Party Contracts as of the Effective Date. Contractor shall be responsible for obtaining all Required Consents relating to this Agreement. If Contractor is unable to obtain a Required Consent, Contractor shall implement, subject to the Using Agency's prior approval, alternative approaches as necessary to perform the Services. Contractor shall be responsible for and shall pay all costs associated with this section, including any fees or other charges imposed by the applicable Third Parties as a condition or consequence of their consent (e.g., any transfer, upgrade or similar fees). The Using Agency shall cooperate with Contractor and provide Contractor such assistance in this regard as the Contractor may reasonably request.

2.4. SLAs and Critical Milestones. Commencing on the Effective Date or as otherwise specified in this Agreement, Contractor shall, as set forth in this Agreement: (a) perform the Services in accordance with SLAs and Critical Milestones; and (b) regularly measure and report on its performance against SLAs and Critical Milestones. Contractor shall maintain all data relating to and supporting the measurement of its performance, including performance against SLAs and Critical Milestones, in sufficient detail to permit a "bottom up" calculation, analysis and reconstruction of performance reports (including all inclusion and exclusion calculations) throughout the term of this Agreement. Such data shall be made available to the Using Agency in an electronic format reasonably acceptable to the Using Agency upon reasonable request and upon the expiration or termination of this Agreement.

2.5. **Default SLAs, Critical Milestones and Fee Reductions.** Unless otherwise explicitly specified in this Agreement, the Contractor's SLAs, SLA targets, and Critical Milestones shall be those that the Using Agency recognizes as commonly accepted "industry best practices" for Services of similar cost, size, and criticality. For example and without limitation, such SLAs include availability and performance Contractor-Provided Software and hosting-related Services, on-time delivery of Deliverables, response and resolution times of Contractor's service desk. For example and without limitation, such Critical Milestones include significant events in projects such as completion of major Deliverables. Unless otherwise specified in this Agreement, Contractor shall proportionately reduce fees for failing to perform the Services in accordance with applicable SLAs and for failing to timely achieve Critical Milestones, and the Using Agency may withhold that amount of fee reduction from any outstanding Contractor invoice. Except as expressly allowed under this Agreement, any such fee reduction accompanying a failure to meet applicable SLAs or Critical Milestones shall not be the Using Agency's exclusive remedy and shall not preclude the Using Agency from seeking other remedies available to it for a material breach of this Agreement.

2.6. **Standards and Procedures Manual.** Contractor will prepare, update, and maintain a manual ("Standards and Procedures Manual") subject to the Using Agency's review and approval that shall: (a) be based upon ITIL processes and procedures; (b) conform to the Using Agency's standard operating procedures (c) be suitable to assist the Using Agency and the Using Agency's auditors in verifying and auditing the Contractor's performance of the Services; and (d) detail the operational and management processes by which Contractor will perform the Services under this Agreement, including to the extent applicable, processes relating to: (i) Change Management and Change control; (ii) Incident management; (iii) Problem management; (iv) configuration management; (v) backup and restore; (vi) capacity management and full utilization of resources; (vii) project management; (viii) management information; (ix) security processes; (x) Contractor's Business Continuity Plan; (xi) Contractor's Disaster Recovery Plan; and (xi) administration, including invoicing. Where this Agreement assumes that the Using Agency will provide Tier 1 help desk support, the Standards and Procedures Manual shall also include sufficient help desk scripts for the Using Agency to provide such support. Contractor will perform the Services in accordance with the Standards and Procedures Manual; *provided, however,* that the provisions of the Standards and Procedures Manual shall never supersede the provisions of this Agreement.

2.7. **Project Management Methodology.** Contractor shall perform the Services in accordance with an industry-recognized project management methodology and procedures, subject to Using Agency approval. Contractor shall comply with the Using Agency's procedures for tracking progress and documents for the duration of the Agreement, including the submission of weekly or monthly status reports to the Using Agency as the Using Agency may require.

2.8. **Change Management Procedures.** Contractor shall utilize Change Management procedures, subject to Using Agency approval, that conform to ITIL/ITSM to manage, track and report on Changes relating to the Services, including procedures for scheduling maintenance, patching, replacement of assets, and other matters required for proper management of the Services. No Change will be made without the Using Agency's prior written consent (which may be given or withheld in the Using Agency's sole discretion), unless such Change: (a) has no impact on the Services being provided by Contractor; (b) has no impact on the security of the Using Agency Data and the Using Agency systems; and (c) causes no increase in any fees under this Agreement or the Using Agency's retained costs.

2.9. **Resources Necessary for Services.** Except as set forth in this Agreement, Contractor shall provide and be financially responsible for all Equipment, Software, materials, facilities, systems and other

resources needed to perform the Services in accordance with the Agreement.

2.10. Using Agency Resources. Except as explicitly allowed under this Agreement, Contractor shall not use, nor permit any Subcontractor, employee, agent, or other Third Party to use any Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency facilities, or any other Equipment, Software, materials, facilities, systems or other resources that the Using Agency provides or otherwise makes available under this Agreement for any purpose other than the performance of the Services; and Contractor shall do so only upon prior written approval of the Using Agency. Contractor shall not purport to, pledge or charge by way of security any of the aforementioned. Contractor shall keep any Equipment owned or leased by the Using Agency that is under Contractor's or a Contractor Subcontractor's control, secure and, for any such Equipment that is not located at the Using Agency facilities, such Equipment shall be clearly identified as the Using Agency's and separable from Contractor's and Third Parties' property.

2.11. Maintenance of Assets. Contractor shall maintain all Equipment, Software, materials, systems, and other resources utilized predominately or exclusively for performing Services in good condition, less ordinary wear and tear, and in such locations and configurations as to be readily identifiable.

2.12. Service Compatibility. To the extent necessary to provide the Services, Contractor shall ensure that the Services, Contractor-Provided Equipment and Contractor-Provided Software (collectively, the "Contractor Resources") are interoperable with the Using Agency-Provided Equipment, Using Agency-Provided Software and with the Using Agency's other Assets, at no cost beyond that specified in this Agreement and without adversely affecting any systems or services retained by the Using Agency or its Third Party Contractors. In the event of any Problem related to service compatibility where it is not known whether the Problem is caused by Contractor's Assets or by Using Agency's Assets, Contractor shall be responsible for correcting the Problem except to the extent that Contractor can demonstrate, to the Using Agency's satisfaction, that the cause was not due to Contractor Resources or to Contractor's action or inaction.

2.13. Cooperation with Using Agency's Third Party Contractors. Contractor shall cooperate with all Third Party Contractors to coordinate its performance of the Services with the services and systems of such Third Party Contractors. Subject to reasonable confidentiality requirements, such cooperation shall include providing: (a) applicable written information, standards and policies concerning any or all of the systems, data, computing environment, and technology direction used in performing the Services so that the goods and services provided by the Third Party Contractor may work in conjunction with or be integrated with the Services; (b) assistance and support services to such Third Party Contractors; (c) Contractor's quality assurance, its development and performance acceptance testing and the applicable requirements of any necessary interfaces for the Third Party Contractor's work product; (d) applicable written requirements of any necessary modifications to the systems or computing environment; and (e) access to and use of the Contractor's Assets as mutually agreed upon by the Using Agency and Contractor (such agreement not to be unreasonably withheld or delayed) and subject to the Third Party Contractor's agreement to comply with Contractor's applicable standard security policies.

2.14. Procurement Assistance. At any time during the Agreement, Contractor shall, as requested by the Using Agency, reasonably cooperate and assist the Using Agency with any Using Agency procurement relating to any of the Services or replacing the Services, including: (a) providing information, reports and data for use in the Using Agency's procurement or transition to a subsequent Third Party

Contractor; (b) answering Third Parties' and Using Agency's questions regarding the procurement and Services transition; and (c) allowing Third Parties participating in the Using Agency's procurement to perform reasonable, non-disruptive due diligence activities in respect of the relevant Services, including providing reasonable access to Key Personnel.

### **3. WARRANTIES**

3.1. Compliance with Law and Regulations. Contractor represents and warrants that it shall perform its obligations under this Agreement in accordance with all Laws applicable to Contractor and its business, including Laws applicable to the manner in which the Services are performed, including any changes in such Laws. With respect to laws governing data security and privacy, the term 'Contractor Laws' shall include any Laws that would be applicable to Contractor if it, rather than the Using Agency, were the owner or data controller of any of the Using Agency Data in its possession or under its control in connection with the Services. Contractor also represents and warrants that it shall identify, obtain, keep current, and provide for Contractor's inspection, all necessary licenses, approvals, permits, authorizations, visas and the like as may be required from time to time under Contractor Laws for Contractor to perform the Services.

3.2. Non-Infringement. Contractor represents and warrants that it shall perform its responsibilities under this Agreement in a manner that does not infringe any patent, copyright, trademark, trade secret or other proprietary rights of any Third Party.

3.3. Contractor Materials and Third Party Intellectual Property. Contractor represents and warrants that it owns, or is authorized to use, all Contractor Intellectual Property, Contractor IP Materials and Contractor-provided Third Party Intellectual Property.

3.4. Developed Software. Contractor represents and warrants that all Developed Software shall be free from material errors in operation and performance, shall comply with the applicable documentation and specifications in all material respects, for twelve (12) months after the installation, testing and acceptance of such Developed Software by the Using Agency; provided, however, for Developed Software that executes on a monthly or less frequent basis (e.g., quarterly or annual cycle), such warranty period will commence on the date of first execution of such Software. Any repairs made to Developed Software pursuant to this Section shall receive a new twelve (12) month warranty period in accordance with the terms of this Section.

3.5. No Open Source. Contractor represents and warrants that Contractor has not (i) incorporated Open Source Materials into, or combined Open Source Materials with, the Deliverables or Software, (ii) distributed Open Source Materials in conjunction with any Deliverables or Software, or (iii) used Open Source Materials, in such a way that, with respect to the foregoing (i), (ii), or (iii), creates obligations for the Contractor with respect to any material Deliverables or grant, or purport to grant, to any Third Party, any rights or immunities under any material Deliverables (including, but not limited to, using any Open Source Materials that require, as a condition of use, modification and/or distribution of such Open Source Materials that other material Software included in Deliverables incorporated into, derived from or distributed with such Open Source Materials be (A) disclosed or distributed in source code form, (B) be licensed for the purpose of making derivative works, or (C) be redistributable at no charge).

3.6. Access to Using Agency Data. Contractor represents and warrants that Contractor has not and will not prevent, or reasonably fail to allow, for any reason including without limitation late payment or otherwise, the Using Agency's access to and retrieval of Using Agency Data. Contractor

acknowledges that Using Agency Data may be Public Records and that any person who knowingly, without lawful authority and with the intent to defraud any party, public officer, or entity, alters, destroys, defaces, removes, or conceals any Public Record commits a Class 4 felony.

3.7. Viruses. Contractor represents and warrants that it has not knowingly provided, and will not knowingly provide, to the Using Agency in connection with the Services, any Software that uses Illicit Code. Contractor represents and warrants that it has not and will not introduce, invoke or cause to be invoked such Illicit Code in any Using Agency IT environment at any time, including upon expiration or termination of this Agreement for any reason, without the Using Agency's prior written consent. If Contractor discovers that Illicit Code has been introduced into Software residing on Equipment hosted or supported by Contractor, Contractor shall, at no additional charge, (a) immediately undertake to remove such Illicit Code, (b) promptly notify the Using Agency in writing of the introduction, and (c) use reasonable efforts to correct and repair any damage to Using Agency Data or Software caused by such Illicit Code and otherwise assist the Using Agency in mitigating such damage and restoring any affected Service, Software or Equipment.

3.8. Resale of Equipment and Software. If Contractor resells to the Using Agency any Equipment or Software that Contractor purchased from a Third Party, then Contractor, to the extent it is legally able to do so, shall pass through any such Third Party warranties to the Using Agency and reasonably cooperate in enforcing them. Such warranty pass-through will not relieve Contractor from its warranty obligations set forth in this Section.

3.9. Data Security. Contractor warrants and represents that (i) the performance of the Services shall not permit any unauthorized access to or cause any loss or damage to Using Agency Data, Using Agency Intellectual Property, or other Using Agency Confidential Information; and (ii) it complies and shall comply with all Using Agency security policies in place from time to time during the term of this Agreement.

#### 4. INTELLECTUAL PROPERTY

4.1. Using Agency Intellectual Property. The Using Agency retains all right, title and interest in and to all Using Agency Intellectual Property and Using Agency IP Materials. To the extent the Using Agency may grant such license, Contractor is granted a worldwide, fully paid-up, nonexclusive license during the term of this Agreement to use, copy, maintain, modify, enhance and create derivative works of the Using Agency Intellectual Property and Using Agency IP Materials that are necessary for performing the Services, and that are explicitly identified in writing by the Using Agency's Chief Information Officer, for the sole purpose of performing the Services pursuant to this Agreement. Contractor shall not be permitted to use any of the Using Agency Intellectual Property or Using Agency IP Materials for the benefit of any entities other than the Using Agency. Contractor shall cease all use of the Using Agency Intellectual Property and Using Agency IP Materials upon expiration or termination of this Agreement. Upon expiration or termination of this Agreement or relevant Services under this Agreement, Contractor shall return to the Using Agency all the Using Agency Intellectual Property, Using Agency IP Materials and copies thereof possessed by Contractor.

4.2. Developed Intellectual Property. As between the Parties, the Using Agency shall have all right, title and interest in all Developed Intellectual Property. Contractor hereby irrevocably and unconditionally assigns, transfers and conveys to the Using Agency without further consideration all of its right, title and interest in such Developed Intellectual Property, including all rights of patent, copyright,

trade secret or other proprietary rights in such materials, which assignment shall be effective as of the creation of such works without need for any further documentation or action on the part of the Parties. Contractor agrees to execute any documents or take any other actions as may reasonably be necessary, or as the Using Agency may reasonably request, to perfect the Using Agency's ownership of any such Developed Intellectual Property. Contractor shall secure compliance with this Section by any personnel, employees, contractors or other agents of Contractor and its Subcontractors involved directly or indirectly in the performance of Services under this Agreement.

4.3. Contractor Intellectual Property. Contractor retains all right, title and interest in and to Contractor Intellectual Property and Contractor IP Materials that Contractor developed before or independently of this Agreement. Contractor grants to the Using Agency, a fully-paid, royalty-free, non-exclusive, non-transferable, worldwide, irrevocable, perpetual, assignable license to make, have made, use, reproduce, distribute, modify, publicly display, publicly perform, digitally perform, transmit, copy, and create derivative works based upon Contractor Intellectual Property and Contractor IP Materials, in any media now known or hereafter known, to the extent the same are embodied in the Services and Deliverables, or otherwise required to exploit the Services or Deliverables. During the term of this Agreement and immediately upon any expiration or termination thereof for any reason, Contractor will provide to the Using Agency the most current copies of any Contractor IP Materials to which the Using Agency has rights pursuant to the foregoing, including any related documentation. Contractor bears the burden to prove that Intellectual Property and IP Materials related to this Agreement were not created under this Agreement.

4.4. Third Party Intellectual Property. Contractor shall not introduce into the Using Agency's environment any Third Party Intellectual Property or otherwise use such Third Party Intellectual Property to perform the Services without first obtaining the prior written consent from the Using Agency's Chief Information Officer, which the Using Agency may give or withhold in its sole discretion. A decision by the Using Agency to withhold its consent shall not relieve Contractor of any obligation to perform the Services.

4.5. Residual Knowledge. Nothing contained in this Agreement shall restrict either Contractor or Using Agency from the use of any ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques relating to the Services which either Contractor or Using Agency, individually or jointly, develops or discloses under this Agreement, provided that in doing so Contractor or Using Agency does not breach its respective obligations under Section 5 relating to confidentiality and non-disclosure and does not infringe the Intellectual Property rights of the other or Third Parties who have licensed or provided materials to the other. Except for the license rights contained under Section 4, neither this Agreement nor any disclosure made hereunder grants any license to either Contractor or Using Agency under any Intellectual Property rights of the other.

4.6. Software Licenses. This Agreement contains all terms and conditions relating to all licenses in Contractor-Provided Software and Contractor IP Materials. Except as explicitly set forth elsewhere in this Agreement, all licenses that Contractor grants in Contractor-Provided Software include the right of use by Third Party Contractors for the benefit of the Using Agency, the right to make backup copies for backup purposes or as may be required by the Using Agency's Business Continuity Plan or Disaster Recovery Plan, the right to reasonably approve the procedures by which Contractor may audit the use of license entitlements, and the right to give reasonable approval before Contractor changes Contractor-Provided Software in a manner that materially and negatively impacts the Using Agency.

## 5. USING AGENCY DATA AND CONFIDENTIALITY

5.1. Property of Using Agency. All Using Agency Confidential Information, including without limitation Using Agency Data, shall be and remain the sole property of the Using Agency. Contractor shall not utilize the Using Agency Data or any other Using Agency Confidential Information for any purpose other than that of performing the Services under this Agreement. Contractor shall not, and Contractor shall ensure that its Subcontractors, its employees, or agents do not, possess or assert any lien or other right against or to the Using Agency Data or any other Using Agency Confidential Information. Without the Using Agency's express written permission, which the Using Agency may give or withhold in its sole discretion, no Using Agency Data nor any other Using Agency Confidential Information, or any part thereof, shall be disclosed, shared, sold, assigned, leased, destroyed, altered, withheld, or otherwise restricted of by Contractor or commercially exploited by or on behalf of Contractor, its employees, Subcontractors or agents.

5.2. Acknowledgment of Importance of Using Agency Confidential Information. Contractor acknowledges the importance of Using Agency Confidential Information, including without limitation Using Agency Data, to the Using Agency and, where applicable, Third Party proprietors of such information, and recognizes that the Using Agency and/or Third Party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement.

5.3. Return of Using Agency Data and Other Using Agency Confidential Information. Upon the Using Agency's request, at any time during this Agreement or at termination or expiration of this Agreement, Contractor shall promptly return any and all requested Using Agency Data and all other requested Using Agency Confidential Information to the Using Agency or its designee in such a format as the Using Agency may reasonably request. Contractor shall also provide sufficient information requested by the Using Agency about the format and structure of the Using Agency Data to enable such data to be used in substantially the manner in which Contractor utilized such data. Also upon Using Agency's request, in lieu of return or in addition to return, Contractor shall destroy Using Agency Data and other Using Agency Confidential Information, sanitize any media upon which such the aforementioned resided using a process that meets or exceeds DoD 5220.28-M 3-pass specifications, and provide documentation of same within 10 days of completion, all in compliance with Using Agency's policies and procedures as updated. All other materials which contain Using Agency Data and other Using Agency Confidential Information shall be physically destroyed and shredded in accordance to NIST Special Publication 800-88; and upon Using Agency request, Contractor shall provide Using Agency with a certificate of destruction in compliance with NIST Special Publication 800-88. Contractor shall be relieved from its obligation to perform any Service to the extent the return of any Using Agency Data or other Using Agency Confidential Information at the Using Agency's request under this Section materially impacts Contractor's ability to perform such Service; provided, that Contractor gives the Using Agency notice of the impact of the return and continues to use reasonable efforts to perform.

5.4. Public Records. Contractor will adhere to all Laws governing Public Records located at 50 ILCS 205/1 et seq. and at 44 Ill. Admin. Code 4500.10 et seq. Specifically, and without limitation, Contractor shall: (a) store Using Agency Data in such a way that each record is individually accessible for the length of the Using Agency's scheduled retention; (b) retain a minimum of two total copies of all Using Agency Data; (c) retain Using Agency Data according to industry best practices for geographic redundancy, such as NIST Special Publication 800-34 as revised; (d) store and access Using Agency Data in a manner allowing individual records to maintain their relationships with one another; (e) capture relevant structural, descriptive, and administrative metadata to Using Agency Data at the time a record is created or enters the control of Contractor or its Subcontractors.

5.5. Disclosure Required by Law, Regulation or Court Order. In the event that Contractor is required to disclose Using Agency Data or other Using Agency Confidential Information in accordance with a requirement or request by operation of Law, regulation or court order, Contractor shall, except to the extent prohibited by law: (a) advise the Using Agency thereof prior to disclosure; (b) take such steps to limit the extent of the disclosure to the extent lawful and reasonably practical; (c) afford the Using Agency a reasonable opportunity to intervene in the proceedings; and (d) comply with the Using Agency's requests as to the manner and terms of any such disclosure.

5.6. Loss of Using Agency Confidential Information. Without limiting any rights and responsibilities under Section 7 of these IT Special Conditions, in the event of any disclosure or loss of, or inability to account for, any Using Agency Confidential Information, Contractor shall promptly, at its own expense: (a) notify the Using Agency in writing; (b) take such actions as may be necessary or reasonably requested by the Using Agency to minimize the violation; and (c) cooperate in all reasonable respects with the Using Agency to minimize the violation and any damage resulting therefrom.

5.6. Undertakings With Respect To Personnel. Contractor acknowledges and agrees that it is responsible for the maintenance of the confidentiality of Using Agency Data and other Using Agency Confidential Information by Contractor Personnel.. Without limiting the generality of the foregoing, Contractor shall undertake to inform all Contractor Personnel of Contractor's obligations with respect to Using Agency Data and other Using Agency Confidential Information and shall undertake to ensure that all Contractor Personnel comply with Contractor's obligations with respect to same.

5.7. Background Checks of Contractor Personnel. Whenever the Using Agency deems it reasonably necessary for security reasons, the Using Agency or its designee may conduct, at its expense, criminal and driver history background checks of Contractor Personnel. Contractor and its Subcontractors shall immediately reassign any individual who, in the opinion of the Using Agency, does not pass the background check.

5.8 Contractor Confidential Information. Using Agency shall use at least the same degree of care to prevent disclosing Contractor Confidential Information to Third Parties as Using Agency employs to avoid unauthorized disclosure, publication or dissemination of its Using Agency Confidential Information of like character.

## 6. DATA SECURITY AND PRIVACY

6.1. General Requirement of Confidentiality and Security. It shall be Contractor's obligation to maintain the confidentiality and security of all Using Agency Confidential Information, including without limitation Using Agency Data, in connection with the performance of the Services. Without limiting Contractor's other obligations under this Agreement, Contractor shall implement and/or use network management and maintenance applications and tools and appropriate fraud prevention and detection and encryption technologies to protect the aforementioned; provided that Contractor shall, at a minimum, encrypt all Personal Information in-transit and at-rest. Contractor shall perform all Services utilizing security technologies and techniques and in accordance with industry leading practices and the Using Agency's security policies, procedures and other requirements made available to Contractor in writing, including those relating to the prevention and detection of fraud or other inappropriate use or access of systems and networks.

6.2. General Compliance. Contractor shall comply with all applicable Laws, regulatory requirements and codes of practice in connection with all capturing, processing, storing and disposing of

Personal Information by Contractor pursuant to its obligations under this Agreement and applicable Data Protection Laws and shall not do, or cause or permit to be done, anything that may cause or otherwise result in a breach by the Using Agency of the same. Contractor and all Contractor Personnel shall comply with all the Using Agency policies and procedures regarding data access, privacy and security.

6.3. Security. Contractor shall establish and maintain reasonable and appropriate physical, logical, and administrative safeguards to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information and to protect same against unauthorized or unlawful disclosure, access or processing, accidental loss, destruction or damage. Such safeguards shall be deemed reasonable and appropriate if established and maintained with the more rigorous of: (a) the Using Agency Policies as updated; (b) the security standards employed by Contractor with respect to the protection of its confidential information and trade secrets as updated; (c) security standards provided by Contractor to its other customers at no additional cost to such customers, as updated; or (d) compliance with the then-current NIST 800-series standards and successors thereto or an equivalent, generally accepted, industry-standard security standards series.

6.4. Written Information Security Program. Contractor shall establish and maintain a WISP designed to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information. Contractor's WISP shall include Data Breach procedures and annual Data Breach response exercises. Contractor's WISP shall be reasonably detailed and shall be subject to the Using Agency's reasonable approval.

6.5. Contractor Personnel. Contractor will oblige its Contractor Personnel to comply with applicable Data Protection Laws and to undertake only to collect, process or use any Using Agency Data, Using Agency Intellectual Property, Using Agency Confidential Information, or Personal Information received from or on behalf of the Using Agency for purposes of, and necessary to, performing the Services and not to make the aforementioned available to any Third Parties except as specifically authorized hereunder. Contractor shall ensure that, prior to performing any Services or accessing any Using Agency Data or other Using Agency Confidential Information, all Contractor Personnel who may have access to the aforementioned shall have executed agreements concerning access protection and data/software security consistent with this Agreement.

6.6. Information Access. Contractor shall not attempt to or permit access to any Using Agency Data or other Using Agency Confidential Information by any unauthorized individual or entity. Contractor shall provide each of the Contractor Personnel, Subcontractors and agents only such access as is minimally necessary for such persons/entities to perform the tasks and functions for which they are responsible. Contractor shall, upon request from the Using Agency, provide the Using Agency with an updated list of those Contractor Personnel, Subcontractors and agents having access to Using Agency Data and other Using Agency Confidential Information and the level of such access. Contractor shall maintain written policies that include auditing access levels and terminating access rights for off-boarded Contractor Personnel, Subcontractors and agents.

6.7. Protected Health Information. If Contractor will have access to Personal Health Information in connection with the performance of the Services, Contractor shall execute a Business Associate Agreement in a form provided by the Using Agency.

6.8. Criminal Justice Information. If Contractor will have access to Criminal Justice Information in connection with the performance of the Services, Contractor shall execute an addendum to this

Agreement governing the Contractor's access to such Criminal Justice Information in a form provided by the Using Agency.

6.9. Cardholder Data. If Contractor will have access to Cardholder Data in connection with the performance of the Services, no less than annually, Contractor shall tender to Using Agency a current attestation of compliance signed by a Qualified Security Assessor certified by the Payment Card Industry.

6.10. Encryption Requirement. Contractor shall encrypt all Personal Information and all other Using Agency Confidential Information the disclosure of which would reasonably threaten the confidentiality and security of Using Agency Data. Contractor shall encrypt the aforementioned in motion, at rest and in use in a manner that, at a minimum, adheres to NIST SP 800-111, NIST SP 800-52, NIST SP 800-77 and NIST SP 800-113 encryption standards. Contractor shall not deviate from this encryption requirement without the advance, written approval of the Using Agency's Information Security Office.

6.11. Using Agency Security. Contractor shall notify the Using Agency if it becomes aware of any Using Agency security practices or procedures (or any lack thereof) that Contractor believes do not comport with generally accepted security policies or procedures.

6.12. Contractor as a Data Processor. Contractor understands and acknowledges that, to the extent that performance of its obligations hereunder involves or necessitates the processing of Personal Information, it shall act only on instructions and directions from the Using Agency; *provided, however,* that Contractor shall notify the Using Agency if it receives instructions or directions from the Using Agency that Contractor believes do not comport with generally accepted security policies or procedures and the Using Agency shall determine whether to modify such instructions or have Contractor comply with such instructions unchanged.

6.13. Data Subject Right of Access and Rectification. If the Using Agency is required to provide or rectify information regarding an individual's Personal Information, Contractor will reasonably cooperate with the Using Agency to the full extent necessary to comply with Data Protection Laws. If a request by a data subject is made directly to Contractor, Contractor shall notify the Using Agency of such request as soon as reasonably practicable.

6.14. Security, Privacy and Data Minimization in Software Development Life Cycle. Contractor shall implement an industry-recognized procedure that addresses the security and privacy of Personal Information as part of the software development life cycle in connection with the performance of the Services. Contractor shall implement procedures to minimize the collection of Personal Information and shall, subject to Using Agency's written request to the contrary, minimize the collection of Personal Information.

6.15. Advertising and Sale of Using Agency Data. Nothing in this Agreement shall be construed to limit or prohibit a Using Agency's right to advertise, sell or otherwise distribute Using Agency Data as permitted by the Cook County Code of Ordinances.

## 7. DATA SECURITY BREACH

7.1. Notice to Using Agency. Contractor shall provide to the Using Agency written notice of such Data Security Breach promptly following, and in no event later than one (1) business day following, the discovery or suspicion of the occurrence of a Data Security Breach. Such notice shall summarize in reasonable detail the nature of the Using Agency Data that may have been exposed, and, if applicable,

any persons whose Personal Information may have been affected, or exposed by such Data Security Breach. Contractor shall not make any public announcements relating to such Data Security Breach without the Using Agency's prior written approval.

7.2. Data Breach Responsibilities. If Contractor knows or has reason to know that a Data Security Breach has occurred (or potentially has occurred), Contractor shall: (a) reasonably cooperate with the Using Agency in connection with the investigation of known and suspected Data Security Breaches; (b) perform any corrective actions that are within the scope of the Services; and (c) at the request and under the direction of the Using Agency, take any all other remedial actions that the Using Agency deems necessary or appropriate, including without limitation, providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or not such notice is required by Law.

7.3. Data Breach Exercises. Contractor shall conduct annual Data Breach exercises. Upon Using Agency request, Contractor shall coordinate its exercises with the Using Agency.

7.4. Costs. The costs incurred in connection with Contractor's obligations set forth in Section 7 or Using Agency's obligations under relevant Data Security Laws shall be the responsibility of the Party whose acts or omissions caused or resulted in the Data Security Beach and may include without limitation: (a) the development and delivery of legal notices or reports required by Law, including research and analysis to determine whether such notices or reports may be required; (b) examination and repair of Using Agency Data that may have been altered or damaged in connection with the Data Security Breach, (c) containment, elimination and remediation of the Data Security Breach, and (d) implementation of new or additional security measures reasonably necessary to prevent additional Data Security Breaches; (e) providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or required by Law; (f) the establishment of a toll-free telephone number, email address, and staffing of corresponding communications center where affected persons may receive information relating to the Data Security Breach; (g) the provision of one (1) year of credit monitoring/repair and/or identity restoration/insurance for affected persons.

## 8. AUDIT RIGHTS

8.1. Generally. Contractor and its Subcontractors shall provide access to any records, facilities, personnel, and systems relating to the Services, at any time during standard business hours, to the Using Agency and its internal or external auditors, inspectors and regulators in order to audit, inspect, examine, test, and verify: (a) the availability, integrity and confidentiality of Using Agency Data and examine the systems that process, store, support and transmit Using Agency Data; (b) controls placed in operation by Contractor and its Subcontractors relating to Using Agency Data and any Services; (c) Contractor's disaster recovery and backup/recovery processes and procedures; and (d) Contractor's performance of the Services in accordance with the Agreement. The aforementioned Using Agency audit rights include the Using Agency's right to verify or conduct its own SOC 2 audits.

8.2. Security Audits. Contractor shall perform, at its sole cost and expense, a security audit no less frequently than every twelve (12) months. The security audit shall test Contractor's compliance with security standards and procedures set forth in: (a) this Agreement, (b) the Standards and Procedures Manual, and (c) any security standards and procedures otherwise agreed to by the Parties.

8.3. Service Organization Control (SOC 2), Type II Audits. Contractor shall, at least once annually in the fourth (4<sup>th</sup>) calendar quarter and at its sole cost and expense, provide to the Using Agency

and its auditors a Service Organization Control (SOC 2), Type II report for all locations at which the Using Agency Data is processed or stored.

8.4. Audits Conducted by Contractor. Contractor promptly shall make available to the Using Agency the results of any reviews or audits conducted by Contractor and its Subcontractors, agents or representatives (including internal and external auditors), including SOC 2 audits, relating to Contractor's and its Subcontractors' operating practices and procedures to the extent relevant to the Services or any of Contractor's obligations under the Agreement. To the extent that the results of any such audits reveal deficiencies or issues that impact the Using Agency or the Services, Contractor shall provide the Using Agency with such results promptly following completion thereof.

8.5. Internal Controls. Contractor shall notify the Using Agency prior to modifying any of its internal controls that impact the Using Agency, the Services and/or Using Agency Data and shall demonstrate compliance with this Agreement.

8.6. Subcontractor Agreements. Contractor shall ensure that all agreements with its Subcontractors performing Services under this Agreement contain terms and conditions consistent with the Using Agency's audit rights.

## 9. RIGHT TO EXIT ASSISTANCE

9.1. Payment for Exit Assistance Services. Exit Assistance Services shall be deemed a part of the Services and included within the Contractor's fees under this Agreement, except as otherwise detailed in this Agreement.

9.2. General. Upon Using Agency's request in relation to any termination, regardless of reason, or expiration of the Agreement, in whole or in part, Contractor shall provide the Using Agency and each of its designees Exit Assistance Services. During the Exit Assistance Period, Contractor shall continue to perform the terminated Services except as approved by the Using Agency and included in the Exit Assistance Plan. Contractor's obligation to provide the Exit Assistance Services shall not cease until the Services have been completely transitioned to the Using Agency or the Using Agency's designee(s) to the Using Agency's satisfaction.

9.3. Exit Assistance Period. Contractor shall: (a) commence providing Exit Assistance Services at the Using Agency's request (i) up to six (6) months prior to the expiration of the Agreement, or (ii) in the event of termination of the Agreement or any Services hereunder, promptly following receipt of notice of termination from the Party giving such notice (such date notice is received, the "Termination Notice Date"), and (b) continue to provide the Exit Assistance Services through the effective date of termination or expiration of the Agreement or the applicable terminated Services (as applicable, the "Termination Date") (such period, the "Exit Assistance Period"). At the Using Agency's option, the Exit Assistance Period may be extended for a period of up to twelve (12) months after the Termination Date. The Using Agency shall provide notice regarding its request for Exit Assistance Services at least sixty (60) days prior to the date upon which the Using Agency requests that Contractor commence Exit Assistance Services unless such time is not practicable given the cause of termination.

9.4. Manner of Exit Assistance Services. Contractor shall perform the Exit Assistance Services

in a manner that, to the extent the same is within the reasonable control of Contractor: (a) is in accordance with the Using Agency's reasonable direction; (b) is in cooperation with, and causes its Subcontractors to cooperate with, the Using Agency and the Using Agency's designee(s); (c) supports the efficient and orderly transfer of the terminated Services to the Using Agency; (d) minimizes any impact on the Using Agency's operations; (e) minimizes any internal and Third Party costs incurred by the Using Agency and the Using Agency's designee(s); and (f) minimizes any disruption or deterioration of the terminated Services. Exit Assistance Plan. Contractor shall develop and provide to the Using Agency, subject to the Using Agency's approval and authorization to proceed, an Exit Assistance Plan that shall: (a) describe responsibilities and actions to be taken by Contractor in performing the Exit Assistance Services; (b) describe in detail any Using Agency Responsibilities which are necessary for Contractor to perform the Exit Assistance Services; (c) describe how any transfer of Assets and any novation, assignment or transfer of contracts will be achieved during the Exit Assistance Period; (d) detail the return, and schedule for return, of Using Agency Data and other Using Agency-specific information to be provided; (e) set out the timetable for the transfer of each element of the terminated Services (including key milestones to track the progress); (f) identify a responsible party for each service, task and responsibility to be performed under the Exit Assistance Plan; and (g) specify reasonable acceptance criteria and testing procedures to confirm whether the transfer of the terminated Services has been successfully completed. Following the Using Agency's approval of, and authorization to proceed with the final Exit Assistance Plan, Contractor will perform the Exit Assistance Services in accordance with the Exit Assistance Plan.

9.6. Exit Assistance Management. Within the first thirty (30) days of the Exit Assistance Period, Contractor will appoint a senior project manager to be responsible for, and Contractor's primary point of contact for, the overall performance of the Exit Assistance Services. Upon Using Agency request, Contractor will provide individuals with the required expertise to perform Exit Assistance Services, even if those individuals are not currently performing Services. Contractor will promptly escalate to the Using Agency any failures (or potential failures) regarding the Exit Assistance Services. Contractor will meet weekly with the Using Agency and provide weekly reports describing: the progress of the Exit Assistance Services against the Exit Assistance Plan; any risks encountered during the performance of the Exit Assistance Services; and proposed steps to mitigate such risks. The Using Agency may appoint, during the Exit Assistance Period, a Using Agency designee to be the Using Agency's primary point of contact and/or to operationally manage Contractor during the Exit Assistance Period.

9.7. Removal of Contractor Materials. Contractor shall be responsible at its own expense for de-installation and removal from the Using Agency Facilities any Equipment owned or leased by Contractor that is not being transferred to the Using Agency under the Agreement subject to the Using Agency's reasonable procedures and in a manner that minimizes the adverse impact on the Using Agency. Prior to removing any documents, equipment, software or other material from any Using Agency Facility, Contractor shall provide the Using Agency with reasonable prior written notice identifying the property it intends to remove. Such identification shall be in sufficient detail to apprise the Using Agency of the nature and ownership of such property.

9.8. Using Agency-specific Information. Upon Using Agency's request, Contractor will specifically provide to the Using Agency the following Using Agency Data to relating to the Services: (a) SLA statistics, reports and associated raw data; (b) operational logs; (c) the Standards and Procedures Manual; (d) Incident and Problem logs for at least the previous two (2) years; (e) security features; (f) passwords and password control policies; (g) identification of work planned or in progress as of the Termination Date, including the current status of such work and projects; and (h) any other information relating to the Services or the Using Agency's IT or operating environment which would be required by a

reasonably skilled and experienced Contractor of services to assume and to continue to perform the Services following the Termination Date without disruption or deterioration. This section shall not limit any other rights and duties relating to Using Agency Data.

9.9. Subcontractors and Third Party Contracts. For each contract for which Using Agency has an option to novate or transfer, Contractor will supply the following information upon Using Agency's request: (a) description of the goods or service being provided under the contract; (b) whether the contract exclusively relates to the Services; (c) whether the contract can be assigned, novated or otherwise transferred to the Using Agency or its designee and any restrictions or costs associated with such a transfer; (d) the licenses, rights or permissions granted pursuant to the contract by the Third Party; (e) amounts payable pursuant to the terms of such contract; (f) the remaining term of the contract and termination rights; and (g) contact details of the Third Party. Contractor's agreements with Third Parties that predominantly or exclusively relate to this Agreement shall not include any terms that would restrict such Third Parties from entering into agreements with the Using Agency or its designees as provided herein.

9.10. Knowledge Transfer. As part of the Exit Assistance Services and upon Using Agency's reasonable request, Contractor will provide knowledge transfer services to the Using Agency or the Using Agency's designee to allow the Using Agency or such designee to fully assume, become self-reliant with respect to, and continue without interruption, the provision of the terminated Services. Contractor shall: allow personnel of the Using Agency or the Using Agency's designee to work alongside Contractor Personnel to shadow their role and enable knowledge transfer; answer questions; and explain procedures, tools, utilities, standards and operations used to perform the terminated Services.

9.11. Change Freeze. Unless otherwise approved by the Using Agency or required on an emergency basis to maintain the performance of the Services in accordance with the Performance Standards and SLAs, during the Exit Assistance Period, Contractor will not make or authorize material Changes to: (a) the terminated Services, including to any Equipment, Software or other facilities used to perform the terminated Services; and (b) any contracts entered into by Contractor that relate to the Services (including contracts with Subcontractors).

9.12. Software Licenses. If and as requested by the Using Agency as part of the Exit Assistance Services, Contractor shall: (a) re-assign licenses to the Using Agency or the Using Agency's designee any licenses for which Contractor obtained Required Consents; (b) grant to the Using Agency, effective as of the Termination Date, at no cost to the Using Agency, a license under Contractor's then-current standard license terms made generally available by Contractor to its other commercial customers in and to all Contractor-Provided Software that constitutes generally commercially available Software that was used by Contractor on a dedicated basis to perform the Services and is reasonably required for the continued operation of the supported environment or to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and with respect to such Software, Contractor shall offer to the Using Agency maintenance (including all enhancements and upgrades) at the lesser of a reasonable rate or the rates Contractor offers to other commercial customers for services of a similar nature and scope; (c) grant to the Using Agency, effective as of the Termination Date, a non-exclusive, non-transferable, fully-paid, royalty-free, perpetual, irrevocable, worldwide license following expiration of the Exit Assistance Period in and to all Contractor-Provided Software that does not constitute

generally commercially available Software that is incorporated into the supported environment, which license shall extend only to the use of such Software by the Using Agency or its designee (subject to Contractor's reasonable confidentiality requirements) to continue to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and (d) provide the Using Agency with a copy of the Contractor-Provided Software described in this Section in such media as requested by the Using Agency, together with object code and appropriate documentation.

## **10. MISCELLANEOUS**

10.1. Survival. Sections 1 (Definitions for Special Conditions), 4 (Intellectual Property), 7 (Data Security Breach), and 8 (Audit Rights) shall survive the expiration or termination of this Agreement for a period of five (5) years (and Sections 5 (Using Agency Data and Confidentiality) and 10 (Miscellaneous) shall survive for a period of ten [10] years) from the later of (a) the expiration or termination of this Agreement (including any Exit Assistance Period), or (b) the return or destruction of Using Agency Confidential Information as required by this Agreement.

10.2. No Limitation. The rights and obligations set forth in these IT special conditions exhibit do not limit the rights and obligations set forth in any Articles of the Professional Services Agreement. For the avoidance of doubt, the use of County in the PSA or GC shall expressly include Using Agency and vice versa.

10.3. No Waiver of Tort Immunity. Nothing in this Agreement waives immunity available to the Using Agency under Law, including under the Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/1-101 et seq.

10.4. No Click-Wrap or Incorporated Terms. The Using Agency is not bound by any content on the Contractor's website, in any click-wrap, shrink-wrap, browse-wrap or other similar document, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the Using Agency has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by the County's Chief Procurement Officer.

10.5. Change Requests. Except as otherwise set forth in this Agreement, this Section 10.5 shall govern all Change Requests and Change Orders. If either Party believes that a Change Order is necessary or desirable, such Party shall submit a Change Request to the other. Contractor represents to Using Agency that it has factored into Contractor's fees adequate contingencies for *de minimis* Change Orders. Accordingly, if Change Requests are made, they will be presumed not to impact the fees under this Agreement; provided, however, that if the Change Request consists of other than a *de minimis* deviation from the scope of the Services and/or Deliverables, Contractor shall provide Using Agency with written notification of such other deviation within five (5) business days after receipt of the Change Request. In the event of a Using Agency-initiated Change Request, within five (5) business days of Contractor's receipt of such Change Request, Contractor shall provide to Using Agency a written statement describing in detail: (a) the reasonably anticipated impact on any Services and Deliverables as a result of the Change Request including, without limitation, Changes in Software and Equipment, and (b) the fixed cost or cost estimate for the Change Request. If Licenser submits a Change Request to Customer, such Change Request shall include the information required for a Change Response.

10.6. Change Orders. Any Change Order that increases the cost or scope of the Agreement, or that materially affects the rights or duties of the Parties as set forth the Agreement, must be agreed upon by the Using Agency in a writing executed by the County's Chief Procurement Officer. In all cases, the approval of all Change Requests and issuance of corresponding Change Orders must comply the County's Procurement Code. If either Party rejects the other's Change Request, Contractor shall proceed to fulfill its obligations under this Agreement.

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 8

Identification of Subcontractors/Suppliers/Subconsultant Form

Contract #: 1615-15006

OCPO ONLY:  
Discrimination  
Check Complete

Cook County  
Office of the Chief Procurement Officer  
**Identification of Subcontractor/Supplier/Subconsultant Form**

The Bidder/Proposer/Respondent ("the Contractor") will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form ("ISF") with each Bid, Request for Proposal, and Request for Qualification. The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract. In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

PDP	Bid/RFP/RFO No. 1615-15006	Date 4/25/18
	Total Bid or Proposal Amount \$4,084,311.50	Contract Title: Electronic Monitoring Services
	Contractor: Track Group, Inc.	Subcontractor/Supplier/Subconsultant to be Allpoints Security and Detective, Inc. added or substitute
	Authorized Contact for Contractor: Derek Cassell	Authorized Contact for Subcontractor/Supplier: Sharon Benson Subconsultant:
	Email Address (Contractor): derek.cassell@trackgrp.com	Email Address (Subcontractor): mail@allpointssecurityinc.com
	Company Address (Contractor): 200 E. 5th Ave, Unit 100	Company Address (Subcontractor): 2112 E. 71st Street
	City, State and Zip (Contractor): Naperville, IL 60563	City, State and Zip (Subcontractor): Chicago, IL 60649
	Telephone and Fax (Contractor): 877-260-2010/630-429-2748	Telephone and Fax (Subcontractor): P: 773-955-6700 F: 773-957-9266
	Estimated Start and Completion Dates (Contractor): TBD	Estimated Start and Completion Dates (Subcontractor): TBD

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

Description of Services or Supplies	Total Price of Subcontract for Services or Supplies
24/7/365 Monitoring Center Services	\$264,879 - \$359,100

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract's approved MBE/WBE Utilization Plan must be submitted to the Office of the Contract Compliance.

Track Group, Inc.

Contractor

Peter Poll

Name

Chief Financial Officer

Title

Prime Contractor Signature

4/25/18

Date

Contract 1515-15006B  
Electronic Monitoring Services  
Category 2 - GPS

EXHIBIT 9

Economic Disclosure Statement

**COOK COUNTY  
ECONOMIC DISCLOSURE STATEMENT  
AND EXECUTION DOCUMENT  
INDEX**

<b>Section</b>	<b>Description</b>	<b>Pages</b>
1	Instructions for Completion of EDS	EDS i - ii
2	Certifications	EDS 1–2
3	Economic and Other Disclosures, Affidavit of Child Support Obligations, Disclosure of Ownership Interest and Familial Relationship Disclosure Form	EDS 3 – 12
4	Cook County Affidavit for Wage Theft Ordinance	EDS 13-14
5	Contract and EDS Execution Page	EDS 15-17

**SECTION 1**  
**INSTRUCTIONS FOR COMPLETION OF**  
**ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT**

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every Proposer responding to a Request for Proposals, and every Respondent responding to a Request for Qualifications, and others as required by the Chief Procurement Officer. The execution of the EDS shall serve as the execution of a contract awarded by the County. The Chief Procurement Officer reserves the right to request that the Bidder or Proposer, or Respondent provide an updated EDS on an annual basis.

**Definitions.** Terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, as applicable.

*Affiliate* means a person that directly or indirectly through one or more intermediaries, Controls is Controlled by, or is under common Control with the Person specified.

*Applicant* means a person who executes this EDS.

*Bidder* means any person who submits a Bid.

*Code* means the Code of Ordinances, Cook County, Illinois available on municode.com.

*Contract* shall include any written document to make Procurements by or on behalf of Cook County.

*Contractor or Contracting Party* means a person that enters into a Contract with the County.

*Control* means the unfettered authority to directly or indirectly manage governance, administration, work, and all other aspects of a business.

*EDS* means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.

*Joint Venture* means an association of two or more Persons proposing to perform a for-profit business enterprise. Joint Ventures must have an agreement in writing specifying the terms and conditions of the relationship between the partners and their relationship and respective responsibility for the Contract.

*Lobby* or lobbying means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.

*Lobbyist* means any person who lobbies.

*Person* or *Persons* means any individual, corporation, partnership, Joint Venture, trust, association, Limited Liability Company, sole proprietorship or other legal entity.

*Prohibited Acts* means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

*Proposal* means a response to an RFP.

*Proposer* means a person submitting a Proposal.

*Response* means response to an RFQ.

*Respondent* means a person responding to an RFQ.

*RFP* means a Request for Proposals issued pursuant to this Procurement Code.

*RFQ* means a Request for Qualifications issued to obtain the qualifications of interested parties.

**INSTRUCTIONS FOR COMPLETION OF**  
**ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT**

**Section 1: Instructions.** Section 1 sets forth the instructions for completing and executing this EDS.

**Section 2: Certifications.** Section 2 sets forth certifications that are required for contracting parties under the Code and other applicable laws. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

**Section 3: Economic and Other Disclosures Statement.** Section 3 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Applicant to the warranties, representations, agreements and acknowledgements contained therein.

**Required Updates.** The Applicant is required to keep all information provided in this EDS current and accurate. In the event of any change in the information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Applicant shall supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is required.

**Additional Information.** The County's Governmental Ethics and Campaign Financing Ordinances impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions, and the Applicant is expected to comply fully with these ordinances. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit the web-site at cookcountyl.gov/ethics-board-of.

**Authorized Signers of Contract and EDS Execution Page.** If the Applicant is a corporation, the President and Secretary must execute the EDS. In the event that this EDS is executed by someone other than the President, attach hereto a certified copy of that section of the Corporate By-Laws or other authorization by the Corporation, satisfactory to the County that permits the person to execute EDS for said corporation. If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a partnership or joint venture, all partners or joint venturers must execute the EDS, unless one partner or joint venture has been authorized to sign for the partnership or joint venture, in which case, the partnership agreement, resolution or evidence of such authority satisfactory to the Office of the Chief Procurement Officer must be submitted with this Signature Page.

If the Applicant is a member-managed LLC all members must execute the EDS, unless otherwise provided in the operating agreement, resolution or other corporate documents. If the Applicant is a manager-managed LLC, the manager(s) must execute the EDS. The Applicant must attach either a certified copy of the operating agreement, resolution or other authorization, satisfactory to the County, demonstrating such person has the authority to execute the EDS on behalf of the LLC. If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a Sole Proprietorship, the sole proprietor must execute the EDS.

A "Partnership" "Joint Venture" or "Sole Proprietorship" operating under an Assumed Name must be registered with the Illinois county in which it is located, as provided in 805 ILCS 405 (2012), and documentation evidencing registration must be submitted with the EDS.

Effective October 1, 2016 all foreign corporations and LLCs must be registered with the Illinois Secretary of State's Office unless a statutory exemption applies to the applicant. Applicants who are exempt from registering must provide a written statement explaining why they are exempt from registering as a foreign entity with the Illinois Secretary of State's Office.

## SECTION 2

CERTIFICATIONS

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE APPLICANT IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE APPLICANT THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE APPLICANT IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE APPLICANT SHALL BE SUBJECT TO TERMINATION.

## A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

- 1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;
- 2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.*;
- 3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;
- 4) Has been convicted of an act committed, within the State, of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.*;
- 5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;
- 6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;
- 7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or
- 8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in subparagraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20% or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

**THE APPLICANT HEREBY CERTIFIES THAT:** The Applicant has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Applicant has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Applicant would not violate the provisions of such Section or of the Code.

## B. BID-RIGGING OR BID ROTATING

**THE APPLICANT HEREBY CERTIFIES THAT:** *In accordance with 720 ILCS 5/33 E-11, neither the Applicant nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.*

## C. DRUG FREE WORKPLACE ACT

**THE APPLICANT HEREBY CERTIFIES THAT:** The Applicant will provide a drug free workplace, as required by (30 ILCS 580/3).

**D. DELINQUENCY IN PAYMENT OF TAXES**

**THE APPLICANT HEREBY CERTIFIES THAT:** *The Applicant is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-171.*

**E. HUMAN RIGHTS ORDINANCE**

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 et seq.).

**F. ILLINOIS HUMAN RIGHTS ACT**

**THE APPLICANT HEREBY CERTIFIES THAT:** *It is in compliance with the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

**G. INSPECTOR GENERAL (COOK COUNTY CODE, CHAPTER 34, SECTION 34-174 and Section 34-250)**

The Applicant has not willfully failed to cooperate in an investigation by the Cook County Independent Inspector General or to report to the Independent Inspector General any and all information concerning conduct which they know to involve corruption, or other criminal activity, by another county employee or official, which concerns his or her office of employment or County related transaction.

The Applicant has reported directly and without any undue delay any suspected or known fraudulent activity in the County's Procurement process to the Office of the Cook County Inspector General.

**H. CAMPAIGN CONTRIBUTIONS (COOK COUNTY CODE, CHAPTER 2, SECTION 2-585)**

**THE APPLICANT CERTIFIES THAT:** It has read and shall comply with the Cook County's Ordinance concerning campaign contributions, which is codified at Chapter 2, Division 2, Subdivision II, Section 585, and can be read in its entirety at [www.municode.com](http://www.municode.com).

**I. GIFT BAN, (COOK COUNTY CODE, CHAPTER 2, SECTION 2-574)**

**THE APPLICANT CERTIFIES THAT:** It has read and shall comply with the Cook County's Ordinance concerning receiving and soliciting gifts and favors, which is codified at Chapter 2, Division 2, Subdivision II, Section 574, and can be read in its entirety at [www.municode.com](http://www.municode.com).

**J. LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-160;**

Unless expressly waived by the Cook County Board of Commissioners, the Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is annually by the Chief Financial Officer of the County, and shall be posted on the Chief Procurement Officer's website.

The term "Contract" as used in Section 4, 1, of this EDS, specifically excludes contracts with the following:

- 1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United State Internal Revenue Code and recognized under the Illinois State not-for -profit law);
- 2) Community Development Block Grants;
- 3) Cook County Works Department;
- 4) Sheriff's Work Alternative Program; and
- 5) Department of Correction inmates.

**SECTION 3****REQUIRED DISCLOSURES****1. DISCLOSURE OF LOBBYIST CONTACTS**

List all persons that have made lobbying contacts on your behalf with respect to this contract:

Name	Address
N/A	_____
	_____
	_____

**2. LOCAL BUSINESS PREFERENCE STATEMENT (CODE, CHAPTER 34, SECTION 34-230)**

*Local business* means a Person, including a foreign corporation authorized to transact business in Illinois, having a bona fide establishment located within the County at which it is transacting business on the date when a Bid is submitted to the County, and which employs the majority of its regular, full-time work force within the County. A Joint Venture shall constitute a Local Business if one or more Persons that qualify as a "Local Business" hold interests totaling over 50 percent in the Joint Venture, even if the Joint Venture does not, at the time of the Bid submittal, have such a bona fide establishment within the County.

- a) Is Applicant a "Local Business" as defined above?

Yes:  No:

- b) If yes, list business addresses within Cook County:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- c) Does Applicant employ the majority of its regular full-time workforce within Cook County?

Yes:  No:

**3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (CODE, CHAPTER 34, SECTION 34-172)**

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

**All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-5) and complete the Affidavit, based on the instructions in the Affidavit.**

**4. REAL ESTATE OWNERSHIP DISCLOSURES.**

The Applicant must indicate by checking the appropriate provision below and providing all required information that either:

- a) The following is a complete list of all real estate owned by the Applicant in Cook County:

**PERMANENT INDEX NUMBER(S):** \_\_\_\_\_  
\_\_\_\_\_

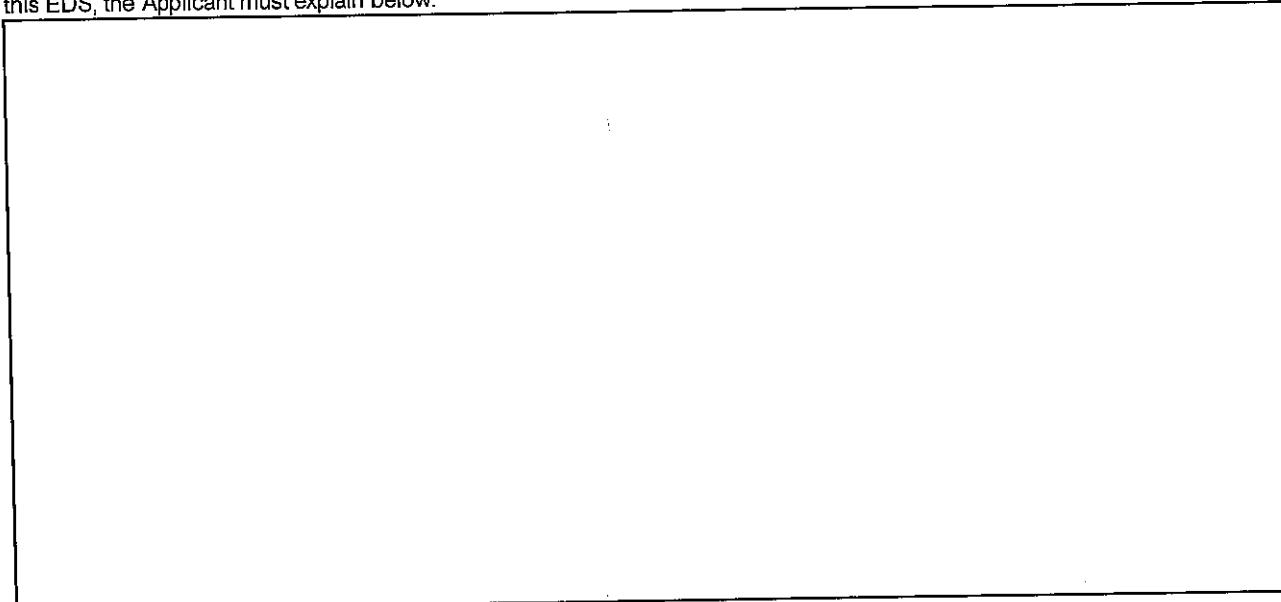
**(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX NUMBERS)**

**OR:**

- b)  The Applicant owns no real estate in Cook County.

**5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.**

If the Applicant is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Applicant must explain below:



If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Applicant certified to all Certifications and other statements contained in this EDS.

**CONTRACT #**

**COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT**

The Cook County Code of Ordinances (§2-610 et seq.) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state **NONE**. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"**Applicant**" means any Entity or person making an application to the County for any County Action.

"**County Action**" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"**Person**" "**Entity**" or "**Legal Entity**" means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by:

1. An Applicant for County Action and
2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

**This Statement is being made by the:**  **Applicant** or  **Stock/Beneficial Interest Holder**

**This Statement is an:**  **Original Statement** or  **Amended Statement**

**Identifying Information:**

**Name:** Track Group, Inc.

**D/B/A:**

**FEIN # Only:** 87-0543981

**Street Address:** 200 E 5th Ave, Suite 100

**City:** Naperville

**State:** IL

**Zip Code:** 60563

**Phone No:** 877-260-2010

**Fax Number:**

**Email:**

**Cook County Business Registration Number:** \_\_\_\_\_  
**(Sole Proprietor, Joint Venture Partnership)**

**Corporate File Number (if applicable):** \_\_\_\_\_

**Form of Legal Entity:**

**Sole Proprietor**  **Partnership**  **Corporation**  **Trustee of Land Trust**

**Business Trust**  **Estate**  **Association**  **Joint Venture**

**Other (describe):** \_\_\_\_\_

**CONTRACT #****Ownership Interest Declaration:**

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest In Applicant/Holder
ETS Limited c/o Mourant Ozannes Corporate Services (Cayman) Limited, 94 Solaris Avenue, Camana Bay, PO Box 1348, Grand Cayman KY1110B, Cayman Islands 40%		
Safety Invest S.A., c/o Nomura International PLC, Nomura PB Nominees LTD, 1 Angel Lane, London EC4R 9AB United Kingdom	15%	

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
ETS Limited ADS Securities	ADS Securities	8th Floor, CI Tower, Corniche Road, P.O. Box 93894, Abu Dhabi, United Arab Emirates

3. Is the Applicant constructively controlled by another person or Legal Entity?  Yes  No  
If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship

**Corporate Officers, Members and Partners Information:**

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
Derek Cassell	200 E 5th Ave, Suite 100, Naperville, IL 60563	Chief Executive Officer	Perpetual
Peter Poll	200 E 5th Ave, Suite 100, Naperville, IL 60563	Chief Financial Officer	Perpetual

**Declaration (check the applicable box):**

- I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.
- I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

**CONTRACT #**

**COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE**

**Peter Poli**

Name of Authorized Applicant/Holder Representative (please print or type)



Signature

peter.poli@trackgrp.com

E-mail address

**Chief Financial Officer**

Title

8 November 2018

Date

877-260-2010

Phone Number

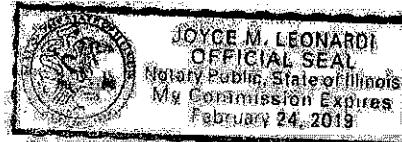
Subscribed to and sworn before me  
this 8 day of Nov. 2018.

My commission expires: 2/24/2019



Notary Public Signature:

Notary Seal



## COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"*Applicant*" means any Entity or person making an application to the County for any County Action.

"*County Action*" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"*Person*" "*Entity*" or "*Legal Entity*" means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and

2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

**This Statement is being made by the**  **Applicant** **or**  **Stock/Beneficial Interest Holder**

**This Statement is an:**  **Original Statement** **or**  **Amended Statement**

**Identifying Information:**

Name ETS Limited

D/B/A: \_\_\_\_\_ FEIN # Only: \_\_\_\_\_

Street Address: c/o Mourant Ozannes Corporate Services (Cayman) Limited, 94 Solaris Avenue, Camana Bay, PO Box 1348

City: Grand Cayman KY11108, Cayman Islands State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Phone No.: \_\_\_\_\_ Fax Number: \_\_\_\_\_ Email: \_\_\_\_\_

Cook County Business Registration Number: \_\_\_\_\_  
(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable): \_\_\_\_\_

**Form of Legal Entity:**

Sole Proprietor  Partnership  Corporation  Trustee of Land Trust

Business Trust  Estate  Association  Joint Venture

Other (describe) \_\_\_\_\_

**Ownership Interest Declaration:**

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
<u>ADS Securities LLC 8th Floor, CI Tower, Corniche Road, P.O. Box 93894, Abu Dhabi, United Arab Emirates 100%</u>		

---



---

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
<u> </u>		

---



---

3. Is the Applicant constructively controlled by another person or Legal Entity? [  ] Yes [  ] No  
If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship
<u>ADS Securities LLC 8th Floor, CI Tower, Corniche Road, P.O. Box 93894, Abu Dhabi, United Arab Emirates 100%</u>			

---



---

**Corporate Officers, Members and Partners Information:**

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
<u>Karim Sehnaoui Address: as listed above in "identifying information" Director Perpetual</u>			
<u>Peter Goulden Address: as listed above in "identifying information" Director Perpetual</u>			

---



---

**Declaration (check the applicable box):**

- I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.
- I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

## COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

Karim Sehnaoui

Name of Authorized Applicant/Holder Representative (please print or type)



Signature

karim.sehnaoui@trackgrp.com

E-mail address

Subscribed to and sworn before me  
this 30th day of April, 2018

Notary Public Signature

Director

Title

04-27-2018

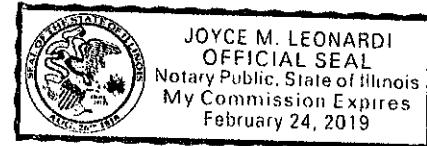
Date

+41 76 30 68 007

Phone Number

My commission expires: 2/24/19

Notary Seal





**COOK COUNTY BOARD OF ETHICS**  
**69 W. WASHINGTON STREET, SUITE 3040**  
**CHICAGO, ILLINOIS 60602**  
**312/603-4304 Office 312/603-9988 Fax**

**FAMILIAL RELATIONSHIP DISCLOSURE PROVISION**

**Nepotism Disclosure Requirement:**

Doing a significant amount of business with the County requires that you disclose to the Board of Ethics the existence of any familial relationships with any County employee or any person holding elective office in the State of Illinois, the County, or in any municipality within the County. The Ethics Ordinance defines a significant amount of business for the purpose of this disclosure requirement as more than \$25,000 in aggregate County leases, contracts, purchases or sales in any calendar year.

If you are unsure of whether the business you do with the County or a County agency will cross this threshold, err on the side of caution by completing the attached familial disclosure form because, among other potential penalties, any person found guilty of failing to make a required disclosure or knowingly filing a false, misleading, or incomplete disclosure will be prohibited from doing any business with the County for a period of three years. The required disclosure should be filed with the Board of Ethics by January 1 of each calendar year in which you are doing business with the County and again with each bid/proposal/quotation to do business with Cook County. The Board of Ethics may assess a late filing fee of \$100 per day after an initial 30-day grace period.

The person that is doing business with the County must disclose his or her familial relationships. If the person on the County lease or contract or purchasing from or selling to the County is a business entity, then the business entity must disclose the familial relationships of the individuals who are and, during the year prior to doing business with the County, were:

- its board of directors,
- its officers,
- its employees or independent contractors responsible for the general administration of the entity,
- its agents authorized to execute documents on behalf of the entity, and
- its employees who directly engage or engaged in doing work with the County on behalf of the entity.

Do not hesitate to contact the Board of Ethics at (312) 603-4304 for assistance in determining the scope of any required familial relationship disclosure.

**Additional Definitions:**

“*Familial relationship*” means a person who is a spouse, domestic partner or civil union partner of a County employee or State, County or municipal official, or any person who is related to such an employee or official, whether by blood, marriage or adoption, as a:

- |                                  |  |                                       |
|----------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Parent  | <input type="checkbox"/> Grandparent     | <input type="checkbox"/> Stepfather   |
| <input type="checkbox"/> Child   | <input type="checkbox"/> Grandchild      | <input type="checkbox"/> Stepmother   |
| <input type="checkbox"/> Brother | <input type="checkbox"/> Father-in-law   | <input type="checkbox"/> Stepson      |
| <input type="checkbox"/> Sister  | <input type="checkbox"/> Mother-in-law   | <input type="checkbox"/> Stepdaughter |
| <input type="checkbox"/> Aunt    | <input type="checkbox"/> Son-in-law      | <input type="checkbox"/> Stepbrother  |
| <input type="checkbox"/> Uncle   | <input type="checkbox"/> Daughter-in-law | <input type="checkbox"/> Stepsister   |
| <input type="checkbox"/> Niece   | <input type="checkbox"/> Brother-in-law  | <input type="checkbox"/> Halfbrother  |
| <input type="checkbox"/> Nephew  | <input type="checkbox"/> Sister-in-law   | <input type="checkbox"/> Halfsister   |

**CONTRACT #**

**COOK COUNTY BOARD OF ETHICS  
FAMILIAL RELATIONSHIP DISCLOSURE FORM**

**A. PERSON DOING OR SEEKING TO DO BUSINESS WITH THE COUNTY**

Name of Person Doing Business with the County: Track Group, Inc.

Address of Person Doing Business with the County: 200 E 5th Ave Unit 100, Naperville, IL 60563

Phone number of Person Doing Business with the County: 877-260-2010

Email address of Person Doing Business with the County: derek.cassell@trackgrp.com

If Person Doing Business with the County is a Business Entity, provide the name, title and contact information for the individual completing this disclosure on behalf of the Person Doing Business with the County:

Derek Cassell, Chief Executive Officer, 877-260-2010, derek.cassell@trackgrp.com

**B. DESCRIPTION OF BUSINESS WITH THE COUNTY**

*Append additional pages as needed and for each County lease, contract, purchase or sale sought and/or obtained during the calendar year of this disclosure (or the proceeding calendar year if disclosure is made on January 1), identify:*

The lease number, contract number, purchase order number, request for proposal number and/or request for qualification number associated with the business you are doing or seeking to do with the County: \_\_\_\_\_

The aggregate dollar value of the business you are doing or seeking to do with the County: \$4,064,311.50

The name, title and contact information for the County official(s) or employee(s) involved in negotiating the business you are doing or seeking to do with the County: Richard Sanchez, Senior Contract Negotiator

The name, title and contact information for the County official(s) or employee(s) involved in managing the business you are doing or seeking to do with the County: Richard Sanchez, Senior Contract Negotiator

**C. DISCLOSURE OF FAMILIAL RELATIONSHIPS WITH COUNTY EMPLOYEES OR STATE, COUNTY OR MUNICIPAL ELECTED OFFICIALS**

*Check the box that applies and provide related information where needed*

- The Person Doing Business with the County is an individual and there is no familial relationship between this individual and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.
- The Person Doing Business with the County is a business entity and there is no familial relationship between any member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity or employees directly engaged in contractual work with the County on behalf of the business entity, and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

**COOK COUNTY BOARD OF ETHICS**  
**FAMILIAL RELATIONSHIP DISCLOSURE FORM**

- The Person Doing Business with the County is an individual and there is a familial relationship between this individual and at least one Cook County employee and/or a person or persons holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County. The familial relationships are as follows:

Name of Individual Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
---	--	--	----------------------------------

_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

*If more space is needed, attach an additional sheet following the above format.*

- The Person Doing Business with the County is a business entity and there is a familial relationship between at least one member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity and/or employees directly engaged in contractual work with the County on behalf of the business entity, on the one hand, and at least one Cook County employee and/or a person holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County, on the other. The familial relationships are as follows:

Name of Member of Board of Director for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
--	--	--	----------------------------------

_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Name of Officer for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
--	--	--	----------------------------------

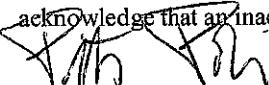
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

**CONTRACT #:**

Name of Person Responsible for the General Administration of the Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
Name of Agent Authorized to Execute Documents for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
Name of Employee of Business Entity Directly Engaged in Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*

*If more space is needed, attach an additional sheet following the above format.*

**VERIFICATION:** To the best of my knowledge, the information I have provided on this disclosure form is accurate and complete. I acknowledge that an inaccurate or incomplete disclosure is punishable by law, including but not limited to fines and debarment.

 Signature of Recipient

- CFO

Date

26 April 2018

**SUBMIT COMPLETED FORM TO:**

Cook County Board of Ethics  
 69 West Washington Street, Suite 3040, Chicago, Illinois 60602  
 Office (312) 603-4304 – Fax (312) 603-9988  
 CookCounty.Ethics@cookcountyl.gov

\* Spouse, domestic partner, civil union partner or parent, child, sibling, aunt, uncle, niece, nephew, grandparent or grandchild by blood, marriage (*i.e.* in laws and step relations) or adoption.

## SECTION 4

**COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE**

Effective May 1, 2015, every Person, *including Substantial Owners*, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"Contract" means any written document to make Procurements by or on behalf of Cook County.

"Person" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"Procurement" means obtaining supplies, equipment, goods, or services of any kind.

"Substantial Owner" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information. **County reserves the right to request additional information to verify veracity of information contained in this Affidavit.**

**I. Contract Information:**

Contract Number: \_\_\_\_\_

County Using Agency (requesting Procurement): **Adult, Juvenile, Sheriff** \_\_\_\_\_

**II. Person/Substantial Owner Information:**

Person (Corporate Entity Name): **Track Group, Inc.** \_\_\_\_\_

Substantial Owner Complete Name: \_\_\_\_\_

FEIN# **87-0543981** \_\_\_\_\_

E-mail address: **derek.cassell@trackgrp.com** \_\_\_\_\_

Street Address: **200 E. 5th Ave, Unit 100** \_\_\_\_\_

City: **Naperville** \_\_\_\_\_ State: **IL** \_\_\_\_\_ Zip: **60563** \_\_\_\_\_

Home Phone: \_\_\_\_\_

**III. Compliance with Wage Laws:**

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

- No *Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq.*,
- No *Illinois Minimum Wage Act, 820 ILCS 105/1 et seq.*,
- No *Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq.*,
- No *Employee Classification Act, 820 ILCS 185/1 et seq.*,
- No *Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq.*,
- No *Any comparable state statute or regulation of any state, which governs the payment of wages*

If the Person/Substantial Owner answered "Yes" to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV**.

**IV. Request for Waiver or Reduction**

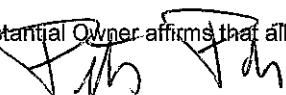
If Person/Substantial Owner answered "Yes" to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction of waiver is made on the basis of one or more of the following actions that have taken place:

- No *There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner*
- No *Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation*
- No *Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default*
- No *Other factors that the Person or Substantial Owner believe are relevant.*

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

**V. Affirmation**

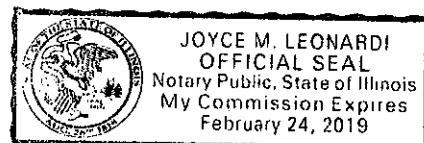
The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

Signature: Date: 26 April 2018Name of Person signing (Print): Peter Poli Title: Chief Financial OfficerSubscribed and sworn to before me this 26<sup>th</sup> day of April, 20 18X Joyce M. Leonard

Notary Public Signature

Notary Seal

Note: The above information is subject to verification prior to the award of the Contract.



## SECTION 4

**COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE**

Effective May 1, 2015, every Person, ***including Substantial Owners***, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"Contract" means any written document to make Procurements by or on behalf of Cook County.

"Person" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"Procurement" means obtaining supplies, equipment, goods, or services of any kind.

"Substantial Owner" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information. **County reserves the right to request additional information to verify veracity of information contained in this Affidavit.**

**I. Contract Information:**

Contract Number: \_\_\_\_\_

County Using Agency (requesting Procurement): \_\_\_\_\_

**II. Person/Substantial Owner Information:**

Person (Corporate Entity Name): Track Group, Inc.

Substantial Owner Complete Name: ETS Limited

FEIN# \_\_\_\_\_

E-mail address: karim.sehnaoui@trackgrp.com

Street Address: c/o Mourant Ozannes Corporate Services (Cayman) Limited, 94 Solaris Avenue, Camana Bay, PO Box 1348

City: Grand Cayman KY11108, Cayman Islands

State: \_\_\_\_\_ Zip: \_\_\_\_\_

Home Phone: ( ) - \_\_\_\_\_

**III. Compliance with Wage Laws:**

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

- No *Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq.,*
- No *Illinois Minimum Wage Act, 820 ILCS 105/1 et seq.,*
- No *Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq.,*
- No *Employee Classification Act, 820 ILCS 185/1 et seq.,*
- No *Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq.,*
- No *Any comparable state statute or regulation of any state, which governs the payment of wages*

If the Person/Substantial Owner answered "Yes" to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV**.

**IV. Request for Waiver or Reduction**

If Person/Substantial Owner answered "Yes" to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction or waiver is made on the basis of one or more of the following actions that have taken place:

- No *There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner*
- No *Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation*
- No *Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default*
- No *Other factors that the Person or Substantial Owner believe are relevant.*

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

**V. Affirmation**

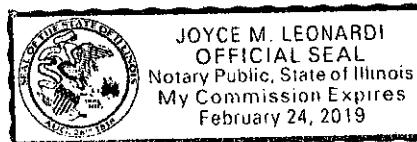
The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

Signature: KSSDate: 04-27-2018Name of Person signing (Print): Karim SehnaouiTitle: DirectorSubscribed and sworn to before me this 30<sup>th</sup> day of April, 20 18x Joyce M. Leonardi

Notary Public Signature

Notary Seal

Note: The above information is subject to verification prior to the award of the Contract.



## SECTION 5

**CONTRACT AND EDS EXECUTION PAGE**  
**PLEASE EXECUTE THREE ORIGINAL PAGES OF EDS**

The Applicant hereby certifies and warrants that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Applicant is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Applicant with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Applicant in this EDS are true, complete and correct. The Applicant agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

**Execution by Corporation**

Track Group, Inc.

Corporation's Name

877-260-2010

Telephone

Jessielee Reeves

Secretary Signature

PETER PoliPtth Ph

President's Printed Name and Signature

peter.poli@trackgrp.com

Email

26 April 2018

Date

**Execution by LLC**

LLC Name

\*Member/Manager Printed Name and Signature

Date

Telephone and Email

**Execution by Partnership/Joint Venture**

Partnership/Joint Venture Name

\*Partner/Joint Venturer Printed Name and Signature

Date

Telephone and Email

**Execution by Sole Proprietorship**

Printed Name Signature

Assumed Name (if applicable)

Date

Telephone and Email

Subscribed and sworn to before me this

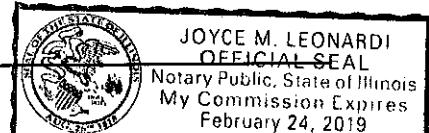
26<sup>th</sup> day of April, 2018Joyce M. Leonardi

Notary Public Signature

My commission expires:

2/24/2019

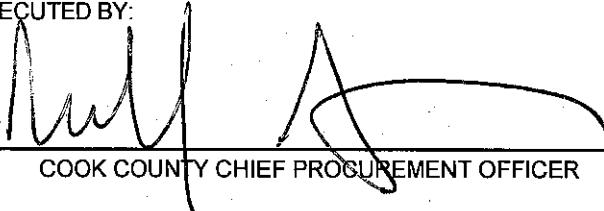
Notary Seal



\*If the operating agreement, partnership agreement or governing documents requiring execution by multiple members, managers, partners, or joint venturers, please complete and execute additional Contract and EDS Execution Pages.

SECTION 6  
COOK COUNTY SIGNATURE PAGE

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS HEREBY EXECUTED BY:

  
COOK COUNTY CHIEF PROCUREMENT OFFICER

DATED AT CHICAGO, ILLINOIS THIS 28<sup>th</sup> DAY OF January, 2019

APPROVED AS TO FORM:



ASSISTANT STATES ATTORNEY  
(Required on contracts over \$1,000,000.00)

CONTRACT TERM & AMOUNT

1515-15006B

CONTRACT #

January 28, 2019 - January 27, 2022

Two (2) one-year renewal options

ORIGINAL CONTRACT TERM

RENEWAL OPTIONS (If Applicable)

\$4,064,311.50

CONTRACT AMOUNT

January 24, 2019

COOK COUNTY BOARD APPROVAL DATE (If Applicable)

APPROVED BY THE BOARD OF  
COOK COUNTY COMMISSIONERS

JAN 24 2019