



Enterprise Service Agreement (ESA)

This Vigilant Solutions Enterprise Service Agreement (the "Agreement") is made and entered into as of this Day of _____, 20__ by and between **Vigilant Solutions, LLC**, a Delaware company, having its principal place of business at 1152 Stealth Street, Livermore, CA 94551 ("Vigilant") and Williamson County, TX on behalf of its Sheriff's Department, a law enforcement agency (LEA) or other governmental agency, having its principal place of business at 508 S. Rock St. Georgetown, TX 78626 ("Customer").

WHEREAS, Vigilant designs, develops, licenses and services advanced video analysis software technologies for law enforcement and security markets;

WHEREAS, Customer desires to license from and receive service for the Hardware and Software Products provided by Vigilant;

THEREFORE, In consideration of the mutual covenants contained herein this Agreement, Customer and Vigilant hereby agree as follows:

I. Definitions:

"CJIS Security Policy" means the FBI CJIS Security Policy document as published by the FBI CJIS Information Security Officer.

"CLK" or **"Camera License Key"** means an electronic key that will permit each license of Vigilant's CarDetector brand LPR software (one CLK per camera) to be used with other Vigilant LPR Hardware Products and Software Products.

"Criminal Justice Information Services Division" or "CJIS" means the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJ to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

"Effective Date" means the date set forth in the first paragraph of this Agreement.

"Enterprise License" means a non-exclusive, non-transferable license to install and operate the Software Products, on any applicable media, without quantity or limitation. This Enterprise Service Agreement allows Customer to install the Software Products on an unlimited number of devices in accordance with the selected Service Package, and allow benefits of all rights granted hereunder this Agreement.

"Hardware Products" means Vigilant's Fixed License Plate Recognition Cameras, Camera Brackets and Solar Panels.

"LPR Data" refers to LPR data collected by the Customer and available on LEARN for use by the Customer.

"Service Fee" means the amount due from Customer prior to the renewal of this Agreement as consideration for the continued use of the Software Products and Service Package benefits according to Section XIII of this Agreement.

SA



“Service Package” means the Customer designated service option which defines the extent of use of the Software Products, in conjunction with any service and/or benefits therein granted as rights hereunder this Agreement. **“Service Period”** has the meaning set forth in Section III (A) of this Agreement.

“Software Products” means Vigilant’s Software Suite including CarDetector, LEARN, and other software applications considered by Vigilant to be applicable for the benefit of security practices.

“Technical Support Agents” means Customer’s staff person responsible for administering the Software Products and acting as Customer’s Software Products support contact.

“User License” means a non-exclusive, non-transferable license to install and operate the Software Products, on any applicable media, limited to a single licensee.

“Users” refers to individuals who are agents of the Customer and who are authorized by the Customer to access LEARN on behalf of Customer through login credentials provided by Customer.

II. Enterprise License Grant; Duplication and Distribution Rights:

Subject to the terms and conditions of this Agreement, Vigilant hereby grants Customer an Enterprise License to the Software Products for the Term provided in Section III below. Except as expressly permitted by this Agreement, Customer or any third party acting on behalf of Customer shall not copy, modify, distribute, loan, lease, resell, sublicense or otherwise transfer any right in the Software Products. Except as expressly permitted by this Agreement, no other rights are granted by implication, estoppels or otherwise. Customer shall not eliminate, bypass, or in any way alter the copyright screen (also known as the “splash” screen) that may appear when Software Products are first started on any computer. Any use or redistribution of Software Products in a manner not explicitly stated in this Agreement, or not agreed to in writing by Vigilant, is strictly prohibited.

III. Term; Termination.

A. Term. The term of this Agreement is five (5) years beginning on the Effective Date unless earlier terminated as provided herein. Vigilant will provide Customer with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a “Service Period”) 60 days prior to the end of the then current Service Period. The first Service Period must be paid in advance. This Agreement and the Enterprise License granted under this Agreement will be extended for a Service Period upon Customer’s payment of that Service Period’s Service Fee, which is due 30 days prior to the expiration of the Service Period, as the case may be. Pursuant to Section VIII below, Customer may also pay in advance for more than one Service Period.

B. Customer Termination. To the extent not in conflict with TEX. CONST. art. III, § 52, if Customer terminates this Agreement for no reason prior to the end of any Service Period, Vigilant will not refund or prorate any license fees paid by the Customer. If Customer’s termination notice is based on an alleged breach by Vigilant, then Vigilant shall have thirty (30) days from the date of receipt of Customer’s notice of termination, which shall set forth in detail Vigilant’s purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Customer Vigilant has not reasonably cured the described breach of this Agreement, Vigilant shall refund to Customer an amount calculated by multiplying the total amount of Service Fees paid by Customer for the then-current Service Period by the percentage resulting



from dividing the number of days remaining in the then-current Service Period, by 365. Upon termination, Customer shall delete all copies of Software Products.

C. Vigilant Termination. Vigilant has the right to terminate this Agreement at any time by providing thirty (30) days written notice to Customer. If Vigilant's termination notice is based on an alleged breach by Customer, then Customer shall have thirty (30) days from the date of its receipt of Vigilant's notice of termination, which shall set forth in detail Customer's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Vigilant Customer has not reasonably cured the described breach of this Agreement, Customer shall immediately discontinue all use of Hardware Products and Software Products and certify to Vigilant that it has returned or destroyed all copies of Software Products in its possession or control. If Vigilant terminates this Agreement prior to the end of a Service Period for no reason, and not based on Customer's failure to cure the breach of a material term or condition of this Agreement, Vigilant shall refund to Customer an amount calculated by multiplying the total amount of Service Fees paid by Customer for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

IV. Warranty and Disclaimer; Infringement Protection; Use of Software Products Interface.

A. Warranty and Disclaimer. Vigilant warrants that the Hardware Products and Software Products will be free from all Significant Defects (as defined below) during the term of this Agreement (the "Warranty Period"). "Significant Defect" means a defect in a Hardware Product or Software Product that impedes the primary function of the Hardware Product or Software Product. This warranty does not include products not manufactured by Vigilant. Vigilant will repair or replace any Hardware Product or Software Product with a Significant Defect during the Warranty Period; *provided, however*, if Vigilant cannot substantially correct a Significant Defect in a commercially reasonable manner, Customer may terminate this Agreement and Vigilant shall refund to Customer an amount calculated by multiplying the total amount of Service Fees paid by Customer for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365. The foregoing remedies are Customer's exclusive remedy for defects in the Software Product. Vigilant shall not be responsible for labor charges for removal or reinstallation of defective Hardware Products or Software Products, charges for transportation, shipping or handling loss, unless such charges are due to Vigilant's gross negligence or intentional misconduct. Vigilant disclaims all warranties, expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall Vigilant be liable for any damages whatsoever arising out of the use of, or inability to use, the Hardware Products and Software Products.

B. Infringement Protection. If an infringement claim is made against Customer by a third-party in a court of competent jurisdiction regarding Customer's use of any of the Hardware Products or Software Products, Vigilant shall indemnify Customer, and assume all legal responsibility and costs to contest any such claim. If Customer's use of any portion of the Hardware Products or Software Products or documentation provided to Customer by Vigilant in connection with the Hardware Products or Software Products is enjoined by a court of competent jurisdiction, Vigilant shall do one of the following at its option and expense within sixty (60) days of such injunction: (1) Procure for Customer the right to use such infringing portion; (2) replace such infringing portion with a non-infringing portion providing equivalent functionality; or (3) modify the infringing portion so as to eliminate the infringement while providing equivalent functionality.

SA



C. Use of Software Products Interface. Under certain circumstances, it may be dangerous to operate a moving vehicle while attempting to operate a touch screen or laptop screen and any of their applications. It is agreed by Customer that Customer's users will be instructed to only utilize the interface to the Software Products at times when it is safe to do so. Vigilant is not liable for any accident caused by a result of distraction such as from viewing the screen while operating a moving vehicle.

V. Software Support, Warranty and Maintenance.

Customer will receive technical support by submitting a support ticket to Vigilant's company support website or by sending an email to Vigilant's support team. Updates, patches and bug fixes of the Software Products will be made available to Customer at no additional charge, although charges may be assessed if the Software Product is requested to be delivered on physical media. Vigilant will provide Software Products support to Customer's Technical Support Agents through e-mail, fax and telephone. Customer allows Vigilant Solutions to access the L5Q camera settings for the purposes of optimizing the plate collection process.

VI. Camera License Keys (CLKs).

Customer is entitled to use of the Software Products during the term of this Agreement to set up and install the Software Products on an unlimited number of media centers within Customer's network in accordance with selected Service Options. As Customer installs additional units of the Hardware Products or Software Products, Customer is required to obtain a Camera License Key (CLK) for each camera installed and considered in active service. A CLK can be obtained by Customer by going to Vigilant's company support website and completing the online request form to Vigilant technical support staff. Within two (2) business days of Customer's application for a CLK, Customer's Technical Support Agent will receive the requested CLK that is set to expire on the last day of the then-current Service Period.

VII. Ownership.

A. Ownership of Software Products. The Software Products are copyrighted by Vigilant and remain the property of Vigilant. The license granted under this Agreement is not a sale of the Software Products or any copy. Customer owns the physical media on which the Software Products are installed, but Vigilant retains title and ownership of the Software Products and all other materials included as part of the Software Products.

B. Ownership of Hardware Products. The Hardware Products provided under this agreement remain the property of Vigilant. Customer has no ownership or rights to Hardware Products provided under this Agreement during or after the Term of this Agreement.

C. Rights in Software Products. Vigilant represents and warrants that: (1) it has title to the Software and the authority to grant license to use the Software Products; (2) it has the corporate power and authority and the legal right to grant the licenses contemplated by this Agreement; and (3) it has not and will not enter into agreements and will not take or fail to take action that causes its legal right or ability to grant such licenses to be restricted.

VIII. Data Sharing.

SA



If Customer is a generator of LPR Data, Customer at its option may share its LPR Data with Law Enforcement Agencies who contract with Vigilant. Vigilant will not share any LPR Data generated by the Customer without the permission of the Customer.

IX. Ownership of LPR Data.

Customer retains all rights to LPR Data generated by the Customer. Should Customer terminate agreement with Vigilant, a copy of all LPR Data generated by the Customer will be created and provided to the Customer. After the copy is created, all LPR Data generated by the Customer will be deleted from LEARN at the written request of an authorized representative of the Customer.

X. Data Retention.

LPR Data is governed by the Customer's retention policy. LPR Data that reaches its expiration date will be deleted from LEARN.

XI. Account Access.

A. Eligibility. Customer shall only authorize individuals who satisfy the eligibility requirements of "Users" to access LEARN. Vigilant in its sole discretion may deny access to LEARN to any individual based on such person's failure to satisfy such eligibility requirements. User logins are restricted to employees of the Customer. No User logins may be provided to non-employees of the Customer without the express written consent of Vigilant.

B. Security. Customer shall be responsible for assigning an Agency Manager who in turn will be responsible for assigning to each of Customer's Users a username and password (one per user account). A limited number of User accounts is provided. Customer will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Customer shall notify Vigilant immediately if Customer believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Customer must notify Vigilant immediately if Customer becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

C. CJIS Requirements. Customer certifies that its LEARN users shall comply with the CJIS requirements outlined in Exhibit A.

XII. Service Package, Fees and Payment Provisions.

A. Service Package. This Enterprise License Agreement is based on the following Service Package:

Service Package - Fixed Camera Subscription Service:

- Fixed Camera with Camera Bracket
- Solar Panel
- Hardware warranty for manufacturer defect
- Vigilant Managed/Hosted LPR server LEARN Account
- Unlimited user licensing and upgrades for the following applications:
 - o LEARN and CarDetector

SA



B. Service Fee. Payment of each Service Fee entitles Customer to all rights granted under this Agreement, including without limitation, use of the Hardware Products and Software Products for the relevant Service Period, replacement of CLKs, and access to the updates and releases of the Software Products and associated equipment driver software to allow the Hardware Products and Software Products to remain current and enable the best possible performance. The annual Service Fee due for a particular Service Period is based on the number of current Vigilant issued CLK's at the time of Service Fee invoicing, and which will be used by Customer in the upcoming Service Period. A schedule of Annual Service Fees for years after the first year of this Agreement is shown below:

Annual Service Fee Schedule (multiplied by number of CLK's Issued)			
	Annual Fee Per CLK	\$2,160.00	

Payment of the Service Fee is due thirty (30) days prior to the renewal of the then-current Service Period. All Service Fees are exclusive of any sales, use, value-added or other federal, state or local taxes (excluding taxes based on Vigilant's net income) and Customer agrees to pay any such tax.

C. Advanced Service Fee Payments. Vigilant will accept advanced Service Fee payment on a case by case basis for Customers who wish to lock in the Service Fee rates for subsequent periods at the rates currently in effect, as listed in the table above. If Customer makes advanced Service Fee payments to Vigilant, advanced payments to Vigilant will be applied in full to each subsequent Service Period's Service Fees until the balance of the credits is reduced to a zero balance. System based advanced credits shall be applied to subsequent Service Fees in the amount that entitles Customer continued operation of the designated camera unit systems for the following Service Period until the credits are reduced to a zero balance.

D. Price Adjustment. Vigilant has the right to increase or decrease the annual Service Fee from one Service Period to another after the 5-Year Term; *provided, however*, that in no event will a Service Fee be increased by more than 4% of the prior Service Period's Service Fees. If Vigilant intends to adjust the Service Fee for a subsequent Service Period, it must give Customer notice of the proposed increase on or before the date that Vigilant invoices Customer for the upcoming Service Period.

XIII. Miscellaneous.

A. Limitation of Liability. IN NO EVENT SHALL VIGILANT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES INCLUDING DAMAGES FOR LOSS OF USE, DATA OR PROFIT, ARISING OUT OF OR CONNECTED WITH THE USE OF THE HARDWARE PRODUCTS AND SOFTWARE PRODUCTS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF VIGILANT HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN NO EVENT WILL VIGILANT'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAID BY CUSTOMER TO VIGILANT FOR THE HARDWARE PRODUCTS AND SOFTWARE PRODUCTS LICENSED UNDER THIS AGREEMENT.

B. Confidentiality. Customer acknowledges that Hardware Products and Software Products contain valuable and proprietary information of Vigilant and Customer will not disassemble, decompile or reverse engineer any Hardware Products or Software Products to gain access to confidential information of Vigilant.

SA



C. Assignment. Neither Vigilant nor Customer is permitted to assign this Agreement without the prior written consent of the other party. Any attempted assignment without written consent is void.

D. Complete Agreement. This Agreement constitutes the final and complete agreement between the parties with respect to the subject matter hereof, and supersedes any prior or contemporaneous agreements, written or oral, with respect to such subject matter.

E. Relationship. The relationship created hereby is that of contractor and customer and of licensor and Customer. Nothing herein shall be construed to create a partnership, joint venture, or agency relationship between the parties hereto. Neither party shall have any authority to enter into agreements of any kind on behalf of the other and shall have no power or authority to bind or obligate the other in any manner to any third party. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Each party hereto represents that it is acting on its own behalf and is not acting as an agent for or on behalf of any third party.

F. No Rights in Third Parties. This agreement is entered into for the sole benefit of Vigilant and Customer and their permitted successors, executors, representatives, administrators and assigns. Nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

G. Construction. The headings used in this Agreement are for convenience and ease of reference only, and do not define, limit, augment, or describe the scope, content or intent of this Agreement. Any term referencing time, days or period for performance shall be deemed calendar days and not business days, unless otherwise expressly provided herein.

H. Severability. If any provision of this Agreement shall for any reason be held to be invalid, illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, such provision shall be construed so as to make it enforceable to the greatest extent permitted, such provision shall remain in effect to the greatest extent permitted and the remaining provisions of this Agreement shall remain in full force and effect.

I. Federal Government. Any use, copy or disclosure of Software Products by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided by DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227 (ALT III), as applicable.

J. Right to Audit. Customer, upon thirty (30) days advanced written request to Vigilant, shall have the right to investigate, examine, and audit any and all necessary non-financial books, papers, documents, records and personnel that pertain to this Agreement and any other Sub Agreements.

SA



K. Notices; Authorized Representatives; Technical Support Agents. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. All notices and communications regarding default or termination of this Agreement shall be delivered by hand or sent by certified mail, postage pre-paid and return receipt requested. Either party may from time to time change the notice address set forth below by delivering 30 days advance notice to the other party in accordance with this section setting forth the new address and the date on which it will become effective.

Vigilant Solutions, LLC Attn: Sales Administration 1152 Stealth Street Livermore, CA 94551	Customer: _____ Attn: _____ Address: _____ _____
--	--

L. Authorized Representatives; Technical Support Agents. Customer's Authorized Representative is responsible for administering this Agreement and Customer's Technical Support Agents are responsible for administering the Hardware Products and Software Products and acting as Customer's Hardware Products and Software Products support contact. Either party may from time to time change its Authorized Representative, and Customer may from time to time change its Technical Support Agents, in each case, by delivering 30 days advance notice to the other party in accordance with the notice provisions of this Agreement.

M. No Waiver of Sovereign Immunity or Powers. Nothing in this agreement will be deemed to constitute a waiver of sovereign immunity or powers of Customer, the Williamson County Commissioners Court, or the Williamson County Judge.

N. Texas Law Applicable to Indemnification. All indemnifications or limitations of liability or statutes of limitations shall be to the extent authorized under Texas law and shall follow Texas law without modifying Customer's rights.

O. Texas Prompt Payment Act Compliance. Payment for goods and services shall be governed by Chapter 2251 of the Texas Government Code. An invoice shall be deemed overdue the 31st day after the later of (1) the date Customer receives the goods under the contract; (2) the date the performance of the service under the contract is completed; or (3) the date the Williamson County Auditor receives an invoice for the goods or services. Interest charges for any overdue payments shall be paid by Customer in accordance with Texas Government Code Section 2251.025. More specifically, the rate of interest that shall accrue on a late payment is the rate in effect on September 1 of Customer's fiscal year in which the payment becomes due. The said rate in effect on September 1 shall be equal to the sum of one percent (1%); and (2) the prime rate published in the Wall Street Journal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday.

P. Mediation. The parties agree to use mediation for dispute resolution prior to and formal legal action being taken on this Contract.

Q. Venue and Governing Law. Venue of this contract shall be Williamson County, Texas, and the law of the State of Texas shall govern.

R. Right to Audit. Vigilant agrees that Customer or its duly authorized representatives shall, until the expiration of three (3) years after final payment under this Agreement, have access to and the right to examine and photocopy any and all books, documents, papers and records of Vigilant which are directly pertinent to the services to be performed under this Agreement for the purposes of making audits, examinations, excerpts, and transcriptions. Vigilant agrees that Customer shall have access during normal working hours to all necessary Vigilant facilities and shall be provided adequate and appropriate workspace in order to conduct audits in compliance with the provisions of this section. Customer shall give Vigilant reasonable advance notice of intended audits.

S. Proprietary Information and Texas Public Information Act. All material submitted to Customer shall become public property and subject to the Texas Public Information Act upon receipt. If a Vendor does not desire proprietary information to be disclosed, each page must be clearly identified and marked proprietary at time of submittal or, more preferably, all proprietary information may be placed in a folder or appendix and be clearly identified and marked as being proprietary. Customer will, to the extent allowed by law, endeavor to protect from public disclosure the information that has been identified and marked as proprietary. The final decision as to what information must be disclosed, however, lies with the Texas Attorney General. Failure to clearly identify and mark information as being proprietary as set forth under this provision will result in all unmarked information being deemed non-proprietary and available to the public. For all information that has not been clearly identified and marked as proprietary by the Vendor, Customer may choose to place such information on Customer's website and/or a similar public database without obtaining any type of prior consent from the Vendor. To the extent, if any, that any provision in this contract is in conflict with Tex. Gov't Code 552.001 et seq., as amended (the "Public Information Act"), the same shall be of no force or effect. Furthermore, it is expressly understood and agreed that Williamson County, its officers and employees may request advice, decisions and opinions of the Attorney General of the State of Texas in regard to the application of the Public Information Act to any items or data furnished to Williamson County as to whether or not the same are available to the public. It is further understood that Williamson County's officers and employees shall have the right to rely on the advice, decisions and opinions of the Attorney General, and that Williamson County, its officers and employees shall have no liability or obligation to any party hereto for the disclosure to the public, or to any person or persons, of any items or data furnished to Williamson County by a party hereto, in reliance of any advice, decision or opinion of the Attorney General of the State of Texas.



IN WITNESS WHEREOF, the parties have executed the Agreement as of the Effective Date.

Manufacturer: Vigilant Solutions, LLC

Title: Area Sales Manager

Date: 03/07/22

Signature: *Sam T. Lee*

Customer: Williamson County, TX on behalf of its Sheriff's

Title: _____

Date: _____

Signature: _____



Exhibit A: CJIS Requirements

Vigilant and the Customer agree on the importance of data security, integrity and system availability and that these security objectives will only be achieved through shared responsibility. Vigilant and the Customer agree they will more likely be successful with information security by use of the Vigilant supplied technical controls and client Customer use of those controls; in conjunction with agency and personnel policies to protect the systems, data and privacy.

Vigilant and the Customer agree that Customer owned and FBI-CJIS supplied data in Vigilant systems does not meet the definition of FBI-CJIS provided Criminal Justice Information (CJI). Regardless, Vigilant agrees to treat the Customer-supplied information in Vigilant systems as CJI. Vigilant will strive to meet those technical and administrative controls; ensuring the tools are in place for the proper protection of systems, information and privacy of individuals to the greatest degree possible.

Vigilant and the Customer agree that information obtained or incorporated into Vigilant systems may be associated with records that are sensitive in nature having, tactical, investigative and Personally Identifiable Information. As such, that information will be treated in accordance with applicable laws, policies and regulations governing protection and privacy of this type of data.

Vigilant and the Customer agree that products and services offered by Vigilant are merely an investigative tool to aid the client in the course of their duties and that Vigilant make no claims that direct actions be initiated based solely upon the information responses or analytical results. Further, Vigilant and the Customer agree that the Customer is ultimately responsible for taking the appropriate actions from results, hits, etc. generated by Vigilant products and require ongoing training, human evaluation, verifying the accuracy and currency of the information, and appropriate analysis prior to taking any action.

As such, the parties agree to do the following:

Vigilant:

1. Vigilant has established the use of FBI-CJIS Security Policy as guidance for implementing technical security controls in an effort to meet or exceed those Policy requirements.
2. Vigilant agrees to appoint a CJIS Information Security Officer to act as a conduit to the client Contracting Government Agency, Agency Coordinator, to receive any security policy information and disseminate to the appropriate staff.
3. Vigilant agrees to adhere to FBI-CJIS Security Policy Awareness Training and Personnel Screening standards as required by the Customer.
4. Vigilant agrees, by default, to classify all client supplied data and information related to client owned infrastructure, information systems or communications systems as "Criminal Justice Data". All client information will be treated at the highest level of confidentiality by all Vigilant staff and authorized partners. Vigilant has supporting guidance/policies for staff handling the full life cycle of information in physical or

SA



electronic form and has accompanying disciplinary procedures for unauthorized access, misuse or mishandling of that information.

5. Vigilant will not engage in data mining, commercial sale, unauthorized access and/or use of any of Customer owned data.
6. Vigilant and partners agree to use their formal cyber Incident Response Plan if such event occurs. 7. Vigilant agrees to immediately inform Customer of any cyber incident or data breach, to include DDoS, Malware, Virus, etc. that may impact or harm client data, systems or operations so proper analysis can be performed and client Incident Response Procedures can be initiated.
8. Vigilant will only allow authorized support staff to access the Customer's account or Customer data in support of Customer as permitted by the terms of contracts.
9. Vigilant agrees to use training, policy and procedures to ensure support staff use proper handling, processing, storing, and communication protocols for Customer data.
10. Vigilant agrees to protect client systems and data by monitoring and auditing staff user activity to ensure that it is only within the purview of system application development, system maintenance or the support roles assigned.
11. Vigilant agrees to inform the Customer of any unauthorized, inappropriate use of data or systems. 12. Vigilant will design software applications to facilitate FBI-CJIS compliant information handling, processing, storing, and communication of Customer.
13. Vigilant will advise Customer when any software application or equipment technical controls are not consistent with meeting FBI-CJIS Policy criteria for analysis and due consideration.
14. Vigilant agrees to use the existing Change Management process to sufficiently plan for system or software changes and updates with Rollback Plans.
15. Vigilant agrees to provide technical security controls that only permit authorized user access to Customer owned data and Vigilant systems as intended by the Customer and data owners.
16. Vigilant agrees to meet or exceed the FBI-CJIS Security Policy complex password construction and change rules. 17. Vigilant will only provide access to Vigilant systems and Customer owned information through Customer managed role-based access and applied sharing rules configured by the Customer.
18. Vigilant agrees to provide technical controls with additional levels of user Advanced Authentication in Physically Non-Secure Locations.
19. Vigilant agrees to provide compliant FIPS 140-2 Certified 128-bit encryption to Customer owned data during transport and storage ("data at rest") while in the custody and control of Vigilant.
20. Vigilant agrees to provide firewalls and virus protection to protect networks, storage devices and data. 21. Vigilant agrees to execute archival, purges and/or deletion of data as configured by the data owner. 22. Vigilant agrees to provide auditing and alerting tools within the software applications so Customer can monitor access and activity of Vigilant support staff and Customer users for unauthorized access, disclosure, alteration or misuse of Customer owned data. (Vigilant support staff will only have access when granted by the Customer.)
23. Vigilant will only perform direct support remote access to Customer systems/infrastructure when requested, authorized and physically granted access to the applications/systems by the Customer. This activity will be documented by both parties.
24. Vigilant creates and retains activity transaction logs to enable auditing by the Customer data owners and Vigilant staff.

SA



25. Vigilant agrees to provide physical protection for the equipment-storing Customer data along with additional technical controls to protect physical and logical access to systems and data.
26. Vigilant agrees to participate in any Information or Technical Security Compliance Audit performed by the Customer, state CJIS System Agency or FBI-CJIS Division.
27. Vigilant agrees to perform independent employment background screening for its' staff and participate in additional fingerprint background screening as required by Customer.
28. Vigilant agrees that the Customer owns all Customer contributed data to include "hot-lists", scans, user information etc., is only shared as designated by the client and remains the responsibility and property of the Customer.

Customer:

1. Customer agrees to appoint an Agency Coordinator as a central Point of Contact for all FBI-CJIS Security Policy related matters and to assign staff that are familiar with the contents of the FBI-CJIS Security Policy.
2. Customer agrees to have the Agency Coordinator provide timely updates with specific information regarding any new FBI-CJIS, state or local information security policy requirements that may impact Vigilant compliance or system/application development and, to facilitate obtaining certifications, training, and fingerprint-based background checks as required.
3. Customer agrees to inform Vigilant when any FBI-CJIS Security Awareness Training, personnel background screening or execution of FBI-CJIS Security Addendum Certifications are required.
4. Customer agrees to immediately inform Vigilant of any relevant data breach or cyber incident, to include DDoS, Malware, Virus, etc. that may impact or harm Vigilant systems, operations, business partners and/or other Customers, so proper analysis can be performed, and Incident Response Procedures can be initiated.
5. Customer agrees that they are responsible for the legality and compliance of information recorded, submitted or placed in Vigilant systems and use of that data.
6. Customer agrees that they are responsible for proper equipment operation and placement of equipment.
7. Customer agrees that they are responsible for vetting authorized user access to Vigilant systems with due consideration of providing potential access to non-Customer information.
8. Customer agrees that responsibility and control of persons granted access to purchased Vigilant systems, along with data stored and transmitted via Vigilant systems, is that of the Customer.
9. Customer agrees that they have responsibility for all data security, handling and data protection strategies from point of acquisition, during transport and until submission ("Hotlist upload") into Vigilant systems.
10. Customer agrees to reinforce client staff policies and procedures for secure storage and protection of Vigilant system passwords.
11. Customer agrees to reinforce client staff policies for creating user accounts with only government domain email addresses. Exceptions will be granted in writing.
12. Customer agrees to reinforce client staff policies for not sharing user accounts.
13. Customer agrees to use Vigilant role-based access as designed to foster system security and integrity.
14. Customer agrees that they control, and are responsible for, appropriate use and data storage policies as well as procedures for the data maintained outside the Vigilant systems. This includes when any information is disseminated, extracted or exported out of Vigilant systems.
15. Customer agrees that they control and are responsible for developing policies, procedures and enforcement for applying deletion/purging and dissemination rules to information within and outside the Vigilant systems.

SA



16. Customer agrees that it is their responsibility to ensure data and system protection strategies are accomplished through the tools provided by Vigilant for account and user management features along with audit and alert threshold features.
17. Customer agrees to use the "virtual escorting" security tools provided for managing client system remote access and monitor Vigilant support staff when authorized to assist the client.
18. Customer agrees that the Vigilant designed technical controls and tools will only be effective in conjunction with Customer created policies and procedures that guide user access and appropriate use of the system. 19. Customer agrees that information and services provided through Vigilant products do not provide any actionable information, Customer users are responsible for the validity and accuracy of their data and developing procedures to verify information with the record owner and other systems (NCIC) based upon the potential lead generated.

SA