VIGILANT SOLUTIONS – INVESTIGATIVE DATA PLATFORM
STATE AND LOCAL LAW ENFORCEMENT AGENCY AGREEMENT

This Agreement is made and entered into effective _____________, 2020 (the "**Effective Date**") between Vigilant Solutions, LLC, a Delaware corporation ("**Vigilant**") and the County of Sonoma through the Sonoma County Sheriff's Office, an Originating Agency Identifier (ORI) credentialed law enforcement agency ("**Agency**").

A. Vigilant stores and disseminates to law enforcement agencies publicly and commercially gathered license plate recognition (LPR) data and booking images as a valued added component of the Vigilant law enforcement package of software; and

B. Agency desires to obtain access to Vigilant's Software Service with available publicly and commercially collected LPR data via the Law Enforcement Archival Reporting Network (LEARN) server and publicly and commercially collected booking images via the FaceSearch server; and

C. Agency may separately purchase LPR hardware components from Vigilant and/or its authorized reseller for use with the Software Service (as defined below);

NOW, THEREFORE, in consideration of the mutual agreements contained herein and other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the parties, the parties agree as follows:

1. Definitions.

(a) **Booking Images**. Refers to both LEA Booking Images and Commercial Booking Images.

(b) **Commercial Booking Images**. Refers to images collected by commercial sources and available on the Software Service with a paid subscription.

(c) **Commercial LPR Data**. Refers to LPR data collected by private commercial sources and available on the Software Service with a paid subscription.

(d) **Confidential Information.** Refers to any and all (i) rights of Vigilant associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights and mask works, trademark and trade name rights and similar rights, trade secrets rights, patents, designs, algorithms and other industrial property rights, other intellectual and industrial property and proprietary rights of every kind and nature, whether arising by operation of law, by contract or license, or otherwise; and all registrations, applications, renewals, extensions, combinations, divisions or reissues of the foregoing; (ii) product specifications, data, know-how, formulae, compositions, processes, designs, sketches, photographs, graphs, drawings, samples, inventions and ideas, and past, current and planned research and development; (iii) current and planned manufacturing and distribution methods and processes, customer lists, current and anticipated customer requirements, price lists, market studies, and business plans; (iv) computer software and programs (including object code and source code), database technologies, systems, structures, architectures, processes, improvements, devices, discoveries, concepts, methods, and information of Vigilant; (v) any other information, however documented, of Vigilant that is a trade secret within the meaning of applicable state trade secret law or under other applicable law, including but not limited to the Software Service, the Commercial LPR Data and the Booking Images; (vi) information concerning the business and affairs of Vigilant (which includes historical financial statements, financial projections and budgets, historical and projected sales, capital spending budgets and plans, the names and backgrounds of key personnel, contractors, agents, suppliers and potential suppliers, personnel training techniques and materials, and purchasing methods and techniques, however documented; and (vii) notes, analysis, compilations, studies, summaries and other material prepared by or for Vigilant containing or based, in whole or in part, upon any information included in the foregoing.

(e) **LEA.** Refers to a law enforcement agency.

(f) **LEA Booking Images**. Refers to images collected by LEAs and available on the Software Service for use by other LEAs. LEA Booking Images are freely available to LEAs at no cost and are governed by the contributing LEA's policies.

(g) **LEA LPR Data.** Refers to LPR data collected by LEAs and available on the Software Service for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA's retention policy.

(h) **License Plate Recognition** ("**LPR**"**).** Refers to the process of utilizing cameras, either stationary or mounted on moving vehicles, to capture and interpret images of vehicle license plates.

(i) **LPR Data.** Refers to both LEA LPR Data and Commercial LPR Data.

(j) **Software Service.** Refers to a web based (hosted) suite of software applications consisting of analytical and investigative software located on a physical database server that also hosts LPR Data and Booking Images.

(k) **User.** Refers to an individual who is authorized by Agency to access the Software Service on behalf of Agency through login credentials provided by Agency. Agency may provide login credentials to agents and sworn officers of the agencies listed in Exhibit B.

2. Licensed Access to the Software Service.

(a) **Grant of License.** During the term of this Agreement, Vigilant grants Agency a non-exclusive, non-transferable right and license to access the Software Service for use in accordance with the terms of this Agreement.

(b) **Authorized Use.** Agency is prohibited from accessing the Software Service other than for law enforcement purposes.

(c) **Ownership of Commercial LPR Data, Commercial Booking Images, FaceSearch Software and LEARN Software.** Except for the rights expressly granted by Vigilant to Agency under this Agreement, Vigilant retains all title and rights to the Commercial LPR Data, Commercial Booking Images, FaceSearch Software and the LEARN Software. Nothing contained in this Agreement shall be deemed to convey to Agency or to any other party any ownership interest in or to any LPR Data, Booking Images, FaceSearch Software or LEARN Software.

(d) **Restrictions on Use of Software Service.** Except as expressly permitted under this Agreement, Agency agrees that it shall not, nor will it permit a User or any other party to, without the prior written consent of Vigilant, (i) copy, duplicate or grant permission to the Software Service or any part thereof; (ii) create, attempt to create, or grant permission to the source program and/or object program associated with the Software Service; (iii) decompile, disassemble or reverse engineer any software component of the Software Service for any reason, including, without limitation, to develop functionally similar computer software or services; or (iv) modify, alter or delete any of the copyright notices embedded in or affixed to the copies of any components of the Software Service. Agency shall instruct each User to comply with the preceding restrictions.

(e) **Third Party Software and Data.** If and to the extent that Vigilant incorporates the software and/or data of any third party into the Software Service, including but not limited to the LEA LPR Data, and use of such third party software and/or data is not subject to the terms of a license agreement directly between Agency and the third party licensor, the license of Agency to such third party software and/or data shall be defined and limited by the license granted to Vigilant by such third party and the license to the Software Service granted by Vigilant under this Agreement. Agency specifically acknowledges that the licensors of such third party software and/or data shall retain all ownership rights thereto, and Agency agrees that it shall not (i) decompile, disassemble or reverse engineer such third party software or otherwise use such third party software for any reason except as expressly permitted herein; (ii) reproduce the data therein for purposes other than those specifically permitted under this Agreement; or (iii) modify, alter or delete any of the copyright notices embedded in or affixed to such third party software. Agency shall instruct each User to comply with the preceding restrictions.

(f) Non-Exclusive Licensed Access. Agency acknowledges that the right or ability of Vigilant to license other third parties to use the Software Service is not restricted in any manner by this Agreement, and that it is Vigilant's intention to license a number of other LEAs to use the Software Service. Vigilant shall have no liability to Agency for any such action.

3. Other Matters Relating to Access to Software Service.

(a) Accessibility. The Software Service, LPR Data, Booking Images and associated analytical tools are accessible to LEAs ONLY.

(b) Access to LEA LPR Data. LEA LPR Data is provided as a service to LEAs at no additional charge.

(c) Access to LEA Booking Images. LEA Booking Images are provided as a service to LEAs at no additional charge.

(d) Eligibility. Agency shall only authorize individuals who satisfy the eligibility requirements of "Users" to access the Software Service. Vigilant in its sole discretion may deny Software Service access to any individual based on such person's failure to satisfy such eligibility requirements.

(e) Account Security (Agency Responsibility).

(1) Agency shall be responsible for assigning an account administrator who in turn will be responsible for assigning to each User a username and password (one per user account). An unlimited number of User accounts is provided. Agency 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). Agency shall notify Vigilant immediately if Agency believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Agency must notify Vigilant immediately if Agency becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

(2) User logins are restricted to agents and sworn officers of the agencies listed in Exhibit B. LPR Data must reside within the Software Service and cannot be copied to another system, unless Agency purchases Vigilant's API. Booking Images must reside within the Software Service and cannot be copied to another system, unless Agency purchase Vigilant's API.

(f) Data Sharing. If Agency is a generator as well as a consumer of LEA LPR Data or LEA Booking Images, Agency at its option may share its LEA LPR Data and/or LEA Booking Images with similarly situated LEAs who contract with Vigilant to access the Software Service (for example, LEAs who share LEA LPR Data with other LEAs).

(g) Subscriptions. Software Service software applications, LPR Data and Booking Images are available to Agency and its Users on an annual subscription basis based the size of the agency.

(h) Application Programming Interface (API). Vigilant offers an API whereby Agency may load LPR Data and/or Booking Images and provide for ongoing updating of LPR Data or Booking Images into a third-party system of Agency's choosing. This service is offered as an optional service and in addition to the annual subscription fee described in **Section 3(g)**.

4. Restrictions on Access to Software Service.

(a) Non-Disclosure of Confidential Information. Agency and each User will become privy to Confidential Information during the term of this Agreement. Agency acknowledges that a large part of Vigilant's competitive advantage comes from the collection and analysis of this Confidential Information and Agency's use, except as expressly permitted under this Agreement, and disclosure of any such Confidential Information would cause irreparable damage to Vigilant.

(b) Restrictions. As a result of the sensitive nature of the Confidential Information, Agency agrees, except to the extent expressly permitted under this Agreement, (i) not to use or disclose, directly or indirectly, and not to permit Users to use or disclose, directly or indirectly, any LPR location information obtained through Agency's access to the Software Service or any other Confidential Information; (ii) not to download, copy or reproduce any portion of the LPR Data and/or Booking Images and other Confidential Information; and (iii) not to sell, transfer, license for use or otherwise exploit the LPR Data and or Booking Images and other Confidential Information in any way. Additionally, Agency agrees to take all necessary precautions to protect the Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Confidential Information as Agency would with Agency's own confidential information and to promptly advise Vigilant in writing upon learning of any unauthorized use or disclosure of the Confidential Information.

(c) **Third Party Information.** Agency recognizes that Vigilant has received, and in the future will continue to receive, from LEAs associated with Vigilant their confidential or proprietary information ("**Associated Third Party Confidential Information**"). By way of example, Associated Third Party Confidential Information includes LEA LPR Data and/or LEA Booking Images. Agency agrees, except to the extent expressly permitted by this Agreement, (i) not to use or to disclose to any person, firm, or corporation any Associated Third Party Confidential Information, (ii) not to download, copy, or reproduce any Associated Third Party Confidential Information, and (iii) not to sell, transfer, license for use or otherwise exploit any Associated Third Party Confidential Information. Additionally, Agency agrees to take all necessary precautions to protect the Associated Third Party Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Associated Third Party Confidential Information as Agency would with Agency's own confidential information and to promptly advise Vigilant in writing upon learning of any unauthorized use or disclosure of the Associated Third Party Confidential Information.

(d) **Non-Publication.** Agency shall not create, publish, distribute, or permit any written, electronically transmitted or other form of publicity material that makes reference to the Software Service or this Agreement without first submitting the material to Vigilant and receiving written consent from Vigilant thereto. This restriction is specifically intended to ensure consistency with other media messaging.

(e) **Non-Disparagement.** Agency agrees not to use proprietary materials or information in any manner that is disparaging. This prohibition is specifically intended to preclude Agency from cooperating or otherwise agreeing to allow photographs or screenshots to be taken by any member of the media without the express consent of Vigilant. Agency also agrees not to voluntarily provide ANY information, including interviews, related to Vigilant, its products or its services to any member of the media without the express written consent of Vigilant.

(f) **Manner of Use.** Agency must use its account in a manner that demonstrates integrity, honesty, and common sense.

(g) **Survival of Restrictions and Other Related Matters.**

(1) Agency shall cause each User to comply with the provisions of this **Section 4**.

(2) Agency agrees to notify Vigilant immediately upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this **Section 4** by Agency or any User, and Agency shall reasonably cooperate with Vigilant to regain possession of the Confidential Information, prevent its further unauthorized use, and otherwise prevent any further breaches of this **Section 4**.

(3) Agency agrees that a breach or threatened breach by Agency or a User of any covenant contained in this **Section 4** will cause irreparable damage to Vigilant and that Vigilant could not be made whole by monetary damages. Therefore, Vigilant shall have, in addition to any remedies available at law, the right to seek equitable relief to enforce this Agreement.

(4) No failure or delay by Vigilant in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise of any such right, power or privilege preclude any other or further exercise thereof.

(5) The restrictions set forth in this **Section 4** shall survive the termination of this Agreement for an indefinite period of time.

5. Term and Termination.

(a) Term. The Term of this Agreement shall be for five (5) years from the Effective Date of this Agreement. Sixty (60) days prior to the expiration of the first Service Period (12 months) and each subsequent Service Period, Vigilant will provide Agency with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a "Service Period"). Payment shall be due 30 days prior to the expiration of the then-current Service Period, as the case may be. Agency may also pay in advance for more than one Service Period.

(b) Termination.

(1) Agency may terminate this Agreement upon thirty (30) days prior written notice to Vigilant for any reason. Agency shall not be entitled to a refund of the annual Service Fee for the then-current Service Period, or any portion thereof, if Agency terminates the agreement prior to the end of a Service Period; however, Agency shall not be obligated to pay any Service Fees for subsequent Service Periods.. If Affiliate's termination notice is based on an alleged breach by Vigilant, then Vigilant shall have thirty (30) days from the date of receipt of Agency'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 Agency, Vigilant has not reasonably cured the described breach of this Agreement, Agency shall be entitled to receive a refund of the Service Fee paid prorated for the remaining term.

(2) Vigilant may terminate this Agreement by providing thirty (30) days written notice to Agency for any reason. If Vigilant's termination notice is based on an alleged breach by Agency, then Agency shall have thirty (30) days from the date of its receipt of Vigilant's notice of termination, which shall set forth in detail Agency's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from Vigilant Agency has not reasonably cured the described breach of this Agreement, Agency shall immediately discontinue all use of the LEARN Software Service. If Vigilant terminates this Agreement prior to the end of a Service Period for breach, no refund for any unused Service Fees will be provided. If Vigilant terminates this Agreement prior to the end of a Service Period for no reason, and not based on Agency's failure to cure the breach of a material term or condition of this Agreement, Vigilant shall refund to Agency an amount calculated by multiplying the total amount of Service Fees paid by Agency 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.

(c) Effect of Termination. Upon termination or expiration of this Agreement for any reason, all licensed rights granted in this Agreement will immediately cease to exist and Agency must promptly discontinue all use of the Software Service, erase all LPR Data and/or Booking Images accessed through the Software Service from its computers, including LPR Data and/or Booking Images transferred through an API, and return all copies of any related documentation and other materials.

6. Payment.

(a) Payment Schedule. Payments to Vigilant shall not exceed $270,000 for the Term of this Agreement. Vigilant shall not be entitled to any additional payment All parties agree that annual payments under this agreement shall be as follows:

Year 1	$40,000
Year 2	$50,000
Year 3	$60,000
Year 4	$60,000
Year 5	$60,000
Total	**$270,000**

(b) Payments made under this agreement will be issued directly to LEHR Auto Electric, the sole authorized reseller for Vigilant Solutions, LLC in Sonoma County.

7. Miscellaneous.

(a) Notices. Any notice under this Agreement must be written. Notices must be addressed to the recipient and either (i) hand delivered; (ii) placed in the United States mail, certified, return receipt requested; (iii) deposited with an overnight delivery service; or (iv) sent via e-mail and followed with a copy sent by overnight delivery or regular mail, to the address or e-mail address specified below. Any mailed notice is effective three (3) business days after the date of deposit with the United States Postal Service or the overnight delivery service, as applicable; all other notices are effective upon receipt. A failure of the United States Postal Service to return the certified mail receipt to the dispatcher of such notice will not affect the otherwise valid posting of notice hereunder.

Addresses for all purposes under this Agreement are:

Vigilant Solutions, LLC
Attn: Steve Cintron
1152 Stealth Street
Livermore, California 94551
Telephone: 925-398-2079
E-mail: steve.cintron@vigilantsolutions.com

Sonoma County Sheriff's Office
Attn: Melissa MacDonald
Address: 2796 Ventura Avenue
Santa Rosa, CA 95403
Telephone: 707-565-3922
E-mail: melissa.macdonald@sonoma-county.org

For Process of Payment:
LEHR Auto Electric
Attn: Mike McGee
4707 Northgate Blvd.
Sacramento, California 95834
Telephone: 925-303-9513
E-mail: mmcgee@lehrauto.com

Either party may designate another address for this Agreement by giving the other party at least five (5) business days' advance notice of its address change. A party's attorney may send notices on behalf of that party, but a notice is not effective against a party if sent only to that party's attorney.

(b) Disclaimer. Vigilant makes no express or implied representations or warranties regarding Vigilant's equipment, website, online utilities or their performance, availability, functionality, other than a warranty of merchantability and fitness for the particular purpose of searching for license plate locations in the database and performing other related analytical functions. Any other implied warranties of merchantability or fitness for a particular purpose are expressly disclaimed and excluded.

(c) Limitations of Liability. VIGILANT WILL NOT BE LIABLE FOR AGENCY'S USE OF THE LPR DATA, BOOKING IMAGES OR SOFTWARE SERVICE APPLICATIONS AND WILL NOT BE LIABLE TO AGENCY UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST OF BUSINESS). TO THE EXTENT THE FOREGOING LIMITATION OF LIABILITY IS PROHIBITED OR OTHERWISE UNENFORCEABLE VILIGANT'S CUMULATIVE LIABILITY TO AGENCY ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED $10,000.00.

(d) Independent Contractor Status. Each party will at all times be deemed to be an independent contractor with respect to the subject matter of this Agreement and nothing contained in this Agreement will be deemed or construed in any manner as creating any partnership, joint venture, joint enterprise, single business enterprise, employment, agency, fiduciary or other similar relationship.

(e) Assignment of this Agreement. Agency may not assign its rights or obligations under this Agreement to any party, without the express written consent of Vigilant.

(f) No Exclusivity. Vigilant may at any time, directly or indirectly, engage in similar arrangements with other parties, including parties which may conduct operations in geographic areas in which Agency operates. Additionally, Vigilant reserves the right to provide LPR Data and Booking Images to third-party entities for purposes of promotions, marketing, business development or any other commercially reasonable reason that Vigilant deems necessary and appropriate.

(g) No Reliance. Agency represents that it has independently evaluated this Agreement and is not relying on any representation, guarantee, or statement from Vigilant or any other party, other than as expressly set forth in this Agreement.

(h) Governing Law; Venue. THIS AGREEMENT IS GOVERNED BY AND INTERPRETED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS WITHOUT REGARD TO CONFLICTS-OF-LAWS PRINCIPLES. THE PARTIES HERETO CONSENT THAT VENUE OF ANY ACTION BROUGHT UNDER THIS AGREEMENT WILL BE IN TARRANT COUNTY, TEXAS.

(i) Amendments. Except as otherwise permitted by this Agreement, no amendment to this Agreement or waiver of any right or obligation created by this Agreement will be effective unless it is in writing and signed by both parties. Vigilant's waiver of any breach or default will not constitute a waiver of any other or subsequent breach or default.

(j) Entirety. This Agreement and the Agency's purchase order, setting forth Vigilant's Software Service being purchased by Agency pursuant to this Agreement and the related product code and subscription price, represent the entire agreement between the parties and supersede all prior agreements and communications, oral or written between the parties. Except to the limited extent expressly provided in this **Section 6(k)**, no contrary or additional terms contained in any purchase order or other communication from Agency will be a part of this Agreement.

(k) Force Majeure. Neither party will be liable for failure to perform or delay in performing any obligation under this Agreement if nonperformance is caused by an occurrence beyond the reasonable control of such party and without its fault or negligence such as acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, delays of common carriers, or any other cause beyond the reasonable control of such party.

(l) Severability. If any provision of this Agreement is held to be invalid, illegal or unenforceable for any reason, such invalidity, illegality or unenforceability will not affect any other provisions of this Agreement, and this Agreement will be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

(m) CJIS Requirements. Agency certifies that its LEARN users shall comply with the CJIS requirements outlined in Exhibit A.

(n) Insurance. With respect to performance of work under this Agreement, Vigilant shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain, insurance as described in Exhibit C, which is attached hereto and incorporated herein by this reference.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by persons duly authorized as of the date and year first above written.

Company: Vigilant Solutions, LLC

Authorized Agent: Bill Quinlan

Title: Vice President Sales Operations

Date: ____

Signature: ____

Agency: County of Sonoma

Authorized Agent: Mark Essick

Title: Sheriff-Coroner

Date: ____

Signature: ____

[signature page – Investigative Data Platform
State and Local Law Enforcement Agency Agreement]

Exhibit A: CJIS Requirements

Vigilant and Agency 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 Agency agree they will more likely be successful with information security by use of the Vigilant supplied technical controls and client Agency use of those controls; in conjunction with agency and personnel policies to protect the systems, data and privacy.

Vigilant and Agency agree that Agency 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 Agency-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 Agency 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 Agency 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 Agency agree that Agency 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 Agency.
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 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 Agency 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 Agency 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 Agency's account or Agency data in support of Agency 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 Agency 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 Agency 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 Agency.
13. Vigilant will advise Agency 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 Agency owned data and Vigilant systems as intended by Agency 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 Agency owned information through Agency managed role-based access and applied sharing rules configured by Agency.
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 Agency 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 Agency can monitor access and activity of Vigilant support staff and Agency users for unauthorized access, disclosure, alteration or misuse of Agency owned data. (Vigilant support staff will only have access when granted by Agency.)
23. Vigilant will only perform direct support remote access to Agency systems/infrastructure when requested, authorized and physically granted access to the applications/systems by Agency. This activity will be documented by both parties.
24. Vigilant creates and retains activity transaction logs to enable auditing by Agency data owners and Vigilant staff.
25. Vigilant agrees to provide physical protection for the equipment-storing Agency 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 Agency, 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 Agency.
28. Vigilant agrees that Agency owns all Agency 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 Agency.

Agency:

1. Agency 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. Agency 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. Agency 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. Agency 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 Agencies, so proper analysis can be performed, and Incident Response Procedures can be initiated.
5. Agency 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. Agency agrees that they are responsible for proper equipment operation and placement of equipment.
7. Agency agrees that they are responsible for vetting authorized user access to Vigilant systems with due consideration of providing potential access to non-Agency information.
8. Agency 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 Agency.
9. Agency 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. Agency agrees to reinforce client staff policies and procedures for secure storage and protection of Vigilant system passwords.
11. Agency agrees to reinforce client staff policies for creating user accounts with only government domain email addresses. Exceptions will be granted in writing.
12. Agency agrees to reinforce client staff policies for not sharing user accounts.
13. Agency agrees to use Vigilant role-based access as designed to foster system security and integrity.
14. Agency 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. Agency 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.
16. Agency 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. Agency 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. Agency agrees that the Vigilant designed technical controls and tools will only be effective in conjunction with Agency created policies and procedures that guide user access and appropriate use of the system.
19. Agency agrees that information and services provided through Vigilant products do not provide any actionable information, Agency 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.

Exhibit B: Users

Agency may provide login credentials to agents and sworn officers of the following agencies:

City of Cotati Police Department
City of Petaluma Police Department
City of Rohnert Park Police Department
City of Santa Rosa Police Department
City of Sonoma Police Department
Town of Windsor Police Department
Santa Rosa Junior College Police Department
Sonoma County Sheriff’s Office
Sonoma County Probation Department
Sonoma State University Police
Sonoma County Public Safety Consortium
Sonoma County Auto Theft Task Force
California Highway Patrol staff working as part of the Sonoma County Auto Theft Task Force

Exhibit C

With respect to performance of work under this Agreement, Consultant shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a *Waiver of Insurance Requirements*. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review the required endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Consultant from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

1. Workers Compensation and Employers Liability Insurance

- **a.** Required if Consultant has employees as defined by the Labor Code of the State of California.
- **b.** Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
- **c.** Employers Liability with minimum limits of $1,000,000 per Accident; $1,000,000 Disease per employee; $1,000,000 Disease per policy.
- **d.** *Required Evidence of Insurance*: Certificate of Insurance.

If Consultant currently has no employees as defined by the Labor Code of the State of California, Consultant agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

2. General Liability Insurance

- **a.** Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.
- **b.** Minimum Limits: $1,000,000 per Occurrence; $2,000,000 General Aggregate; $2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.
- **c.** Consultant is solely responsible for any deductible or self-insured retention.
- **d.** County of Sonoma, its Officer, Agents, and Employees, 2796 Ventura Avenue, Santa Rosa, CA 95403, shall be included as additional insureds for liability arising out of operations by or on behalf of the Consultant in the performance of this Agreement on a blanket endorsement.
- **e.** The General Liability insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.
- **f.** The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the "f" definition of insured contract in ISO form CG 00 01, or equivalent).
- **g.** This insurance shall apply separately to each insured against whom claim is made or suit is brought subject to the Contractor's limit of liability.
- **h.** *Required Evidence of Insurance:*
  - **i.** Copy of the blanket additional insured endorsement; and
  - **ii.** Certificate of Insurance.

3. Automobile Liability Insurance

- **a.** Minimum Limit: $1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.
- **b.** Insurance shall cover all owned autos. If Consultant currently owns no autos, Consultant agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.
- **c.** Insurance shall cover hired and non-owned autos.
- **d.** *Required Evidence of Insurance*: Certificate of Insurance.

4. Professional Liability/Errors and Omissions Insurance

- **a.** Minimum Limits: $1,000,000 per claim or per occurrence; $1,000,000 annual aggregate.
- **b.** Consultant shall be solely responsible for any deductible under Consultant's policy.
- **c.** If Consultant's services include: (1) programming, customization, or maintenance of software: or (2) access to individuals' private, personally identifiable information, the insurance shall cover:
  - **i.** Breach of privacy; breach of data; programming errors, failure of work to meet contracted standards, and unauthorized access; and
  - **ii.** Claims against Consultant arising from the negligence of Consultant, Consultant's employees and Consultant's subcontractors.
- **d.** If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
- **e.** Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.
- **f.** *Required Evidence of Insurance*: Certificate of Insurance specifying the limits
- **g.** *Standards for Insurance Compan*ies
  Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

5. Documentation

- **a.** The Certificate of Insurance must include the following reference: Investigative Data Platform Agreement.
- **b.** All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Consultant agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.
- **c.** The name and address for Certificates of Insurance is: County of Sonoma, its Officer, Agents, and Employees, 2796 Ventura Avenue, Santa Rosa, CA 95403.
- **d.** Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.
- **e.** Consultant shall provide immediate written notice if: (1) any of the required insurance policies is terminated;

6. Policy Obligations
Consultant's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

7. Material Breach

If Consultant fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Consultant resulting from said breach. Alternatively, County may purchase the required insurance, and without further notice to Consultant, County may deduct from sums due to Consultant any premium costs advanced by County for such insurance. These remedies shall be in addition to any other remedies available to County.