



County of Santa Clara

Office of the County Executive

Procurement Department

150 W. Tasman Drive

San Jose, CA 95134

Telephone 408-491-7400 • Fax 408-491-7496

FIRST AMENDMENT TO AGREEMENT NO. CW2231610 BY AND BETWEEN THE COUNTY OF SANTA CLARA AND FORENSIC LOGIC LLC

This is the First Amendment to the Agreement between the County of Santa Clara (County) and Forensic Logic, LLC ("Contractor") originally entered into on December 21, 2018 to provide COPLINK Detect and LEAP Search Subscription Services for the County.

On August 11, 2020, the Board of Supervisor approved this amendment to the Agreement.

This Agreement is amended as follows effective August 11, 2020:

1. Key Provision, **AGREEMENT TERM**, of the Agreement is revised to read: "This Agreement commences on January 1, 2019 and expires on November 30, 2020 unless terminated earlier or otherwise amended."
2. Key Provision, **TOTAL AGREEMENT VALUE**, is revised to read: "The total not to exceed value of this Agreement is \$521,938, which represents an increase of \$178,258 from the prior not to exceed value of \$343,680."

Contractor understands that this not to exceed value does not represent a commitment by County to Contractor.

3. Add **EXHIBIT C – REMOTE ACCESS**, attached hereto and incorporated herein by this reference.
4. Add **EXHIBIT D – COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES**, attached hereto and incorporated herein by this reference.
5. Add **EXHIBIT E – FBI CJIS SECURITY ADDENDUM**, attached hereto and incorporated herein by this reference.
6. Add **EXHIBIT F – EXECUTED CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT**, attached hereto and incorporated herein by this reference.
7. Add **EXHIBIT G – CLETS EMPLOYEE/VOLUNTEER STATEMENT**, attached hereto and incorporated herein by this reference.
8. Add **APPENDIX 1.1, PRICING SUMMARY**, attached hereto and incorporated herein by this reference.
9. Replace the following provisions in **EXHIBIT A, COUNTY OF SANTA CLARA STANDARD TERMS AND CONDITIONS FOR AGREEMENT FOR INFORMATION TECHNOLOGY GOODS AND RELATED SERVICES**, in their entirety with the following:

Board of Supervisors: Mike Wasserman, Cindy Chavez, Dave Cortese, Susan Ellenberg, S. Joseph Simitian
County Executive: Jeffrey V. Smith

Approved: 08/11/2020

DEFINITIONS

- a. "Agreement" means the Key Provisions, Exhibit A (County of Santa Clara Standard Terms and Conditions for Agreement for Goods and Services), Exhibit B (Forensic Logic Subscription Services Agreement), all Appendices attached to Exhibit B, and any written amendments entered into by the Parties including any exhibits or appendices attached thereto. Exhibit B (Forensic Logic Subscription Services Agreement) and Exhibit B, Appendix I (Order Form) are hereby incorporated by reference into this Agreement. In the event of conflict between Exhibit A (County of Santa Clara Standard Terms and Conditions for Agreement for Goods and Services) and Exhibit B (Subscription Services Agreement), Exhibit A as amended shall prevail.
- b. "Contractor Confidential Information" shall include (i) all material, non-public business and technical information that, if disclosed in writing is marked "CONFIDENTIAL AND PROPRIETARY," or, if disclosed orally, is identified as "CONFIDENTIAL" or "PROPRIETARY" at the time of disclosure, and is summarized in a writing sent to County within thirty (30) days of such disclosure; and (ii) the COPLINK Software;
- c. "County Confidential Information" shall include all material, non-public information (including material, non-public County Data) appearing in any form (including, without limitation, written, oral or displayed), that is disclosed, directly or indirectly, through any means of communication by County, its agents or employees, to Contractor, its agents or employees, or any of its affiliates or representatives.
- d. "County Data" shall mean data and information received by Contractor from County. County Data includes any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a contractor for use by County. As between Contractor and County, all County Data shall remain the property of County.
- e. "County/SBISS Law Enforcement Data" shall mean law enforcement data and information received by Contractor from County and any member agency of the South Bay Information Sharing System ("SBISS"). As between Contractor and County, all County/SBISS Law Enforcement Data shall remain the property of County.
- f. "Deliverables" means goods, services, software, hardware, information technology, telecommunications technology, enhancements, updates, new versions or releases, documentation, and any other items to be delivered pursuant to this Agreement, including any such items furnished incident to the provision of services.
- g. "Documentation" means manuals and other printed materials (including updates and revisions) necessary or useful to the County in its use or maintenance of the Deliverables provided pursuant to this Agreement.

66. CONTRACTOR TRAVEL EXPENSES

Contractor shall be solely responsible for any travel fees or out of pocket expenses

67. INFORMATION SECURITY COMPLIANCE

- A. For purposes of this section and Section 68, the following Definitions will apply:
 - (1) "Breach" means unauthorized access to, or use of, County Data or County/SBISS Law Enforcement Data or information security networks or systems that compromises confidentiality, integrity, and/or availability those systems, County Data, or County/SBISS Law Enforcement Data.
 - (2) "Independent Penetration Testing," or "pen testing," means the County's practice - by using an independent third party - of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit

- (3) "Risk Assessment" means the process by which the County's Information Security Office ("ISO") assesses (i) the Contractor's information security program, and related aspects, by identifying, analyzing, and understanding how the Contractor will store, process and transmit County Data and County/SBISS Law Enforcement Data; and (ii) the potential impact on the County of any security risks, weaknesses and threats related to safeguarding County assets, County Data, and County/SBISS Law Enforcement Data. The Risk Assessment usually includes the ISO's evaluation of documentation provided by the Contractor.

B. Contractor shall do all of the following:

- (1) Maintain or improve upon its information security posture at the time of the County's initial Risk Assessment as reasonably determined by the County. Contractor shall provide written notice to the County's Information Security Office ("ISO") of any changes or deficiencies to its information security posture.
- (2) Protect the confidentiality, integrity, availability of the County's data and comply with any information security requirements provided to Contractor by the ISO for the entire term of the Agreement.
- (3) Follow any updated security requirements for the remaining term of the Agreement if the County re-evaluates the Risk Assessment, conducts periodic audits, and/or completes annual Independent Penetration Testing.
- (4) Upon discovering any Breach that could impact the County, whether caused by Contractor, its officers, employees, contractors or agents or others, the Contractor shall notify the ISO at o365-iso-team@sccconnect.onmicrosoft.com within 24 hours. Contractor shall also comply with all of its other obligations in this Agreement relating to breaches and potential breaches.

68. COUNTY DATA AND COUNTY/SBISS LAW ENFORCEMENT DATA

- (1) Contractor shall not acquire any ownership interest in County Data (including County Confidential Information) or County/SBISS Law Enforcement Data. As between Contractor and County, all County Confidential Information, County Data, and/or County/SBISS Law Enforcement Data shall remain the property of the County. Contractor shall not, without County's written permission, use or disclose County Data (including County Confidential Information) or County/SBISS Law Enforcement Data other than in the performance of its obligations under this Agreement. The foregoing obligation will not restrict Contractor from disclosing County Confidential Information (a) pursuant to the order or requirement of a court, administrative agency, or other governmental body, provided that Contractor gives reasonable notice to County to contest such order or requirement prior to disclosure; (b) as required under applicable securities regulations, provided that Contractor gives reasonable notice to County to contest such order or requirement prior to disclosure; or (c) on a confidential basis to its legal or financial advisors, provided Contractor gives reasonable notice to County to contest such disclosure prior to disclosure as necessary pursuant to (a) and (b).
- (2) Contractor is authorized to share County/SBISS Law Enforcement Data stored in COPLINK through LEAP and may make it available to other law enforcement agencies that have access to LEAP within and outside of the SBISS South Bay Region Node, with the following exceptions: (a) data that is deemed sensitive or confidential by the originating agency in COPLINK will be afforded the same restrictions in LEAP; (b) Contractor will not share County/SBISS Law Enforcement Data with the U.S. Department of Homeland Security for civil immigration enforcement purposes; and (c) Contractor will not share Automated License Plate Recognition data with any agency outside the SBISS South Bay Region Node.
- (3) Contractor shall be responsible for establishing and maintaining an information security program that is designed to ensure the security and confidentiality of County Data and County/SBISS Law Enforcement Data, protect against any anticipated threats or hazards to the security or integrity of County Data or County/SBISS Law Enforcement Data, and protect against unauthorized access to

or use of County Data that could result in substantial harm or inconvenience to County or any end users.

- (4) Contractor shall not access, use, or copy for direct or indirect use County Data or County/SBISS Law Enforcement Data after completion or termination of this Agreement without express written consent of County, except as may otherwise be provided for in this Agreement. Upon termination or expiration of this Agreement, Contractor shall seek and follow County's direction regarding the proper disposition of County Data. All County/SBISS Law Enforcement Data, including copies, must be destroyed, including deletion from any electronic medium, within thirty (30) days of expiration or termination of this Agreement or at County's written request, at no cost to the County or to any SBISS member agency. Contractor shall provide County with a declaration under penalty of perjury confirming destruction.
- (5) Contractor shall take appropriate action to address any incident of unauthorized access to County Data or County/SBISS Law Enforcement Data, including addressing and/or remedying the issue that resulted in such unauthorized access, and notifying County by phone or in writing within 24 hours of any incident of unauthorized access to County Data or County/SBISS Law Enforcement Data, or any other breach in Contractor's security that materially affects County or end users. If the initial notification is by phone, Contractor shall provide a written notice within 5 days of the incident. Contractor shall be responsible for ensuring compliance by its officers, employees, agents, and subcontractors with the confidentiality, privacy, and information security requirements of this Agreement. Should County Confidential Information, legally protected County Data, and/or County/SBISS Law Enforcement Data be divulged to unauthorized third parties, Contractor shall comply with all applicable federal and state laws and regulations, including but not limited to California Civil Code sections 1798.29 and 1798.82 at Contractor's sole expense. Contractor shall not charge County for any expenses associated with Contractor's compliance with these obligations.
- (6) Contractor shall comply with all applicable federal and state laws, regulations, and policies governing the confidentiality and security of criminal justice data, including the current Federal Bureau of Investigation's Criminal Justice Information Services ("CJIS") Security Policy and the California Law Enforcement Telecommunications System ("CLETS") Policies, Practices, and Procedures. Contractor recognizes that the misuse of protected County/SBISS Law Enforcement Data may be prosecuted to the full extent of the law.
- (7) Contractor shall defend, indemnify and hold County harmless against any claim, liability, loss, injury or damage arising out of, or in connection with, the unauthorized use, access, and/or disclosure of information by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the County.

10. Add the following provisions to **EXHIBIT A, COUNTY OF SANTA CLARA STANDARD TERMS AND CONDITIONS FOR AGREEMENT FOR INFORMATION TECHNOLOGY GOODS AND RELATED SERVICES**, to read as follows:

71. IMMEDIATE TERMINATION FOR CAUSE

Notwithstanding any other provision in this Agreement:

- (1) Contractor's failure to comply with all terms and conditions set forth in Section 67 (Information Security Compliance), Exhibit C (Remote Access), Exhibit D (User Responsibility Statement for Third Parties), Exhibit E (FBI CJIS Security Addendum), and Exhibit F (Executed CLETS Private Contractor Management Control Agreement), or failure to require such compliance of its officers, employees, contractors and agents ("Contractor's personnel") engaged in performance of this Agreement, shall constitute a material breach of this Agreement and the County may immediately terminate this Agreement for cause.

- (2) Contractor shall not allow Contractor's personnel to perform services for the County unless and until its employees sign Exhibit C (Remote Access) if applicable, Exhibit D (User Responsibility Statement for Third Parties), Exhibit E (FBI CJIS Security Addendum), and Exhibit G (CLETS Employee/Volunteer Statement). If Contractor's personnel access County/SBISS Data or County systems without first signing, that will constitute a material breach of this Agreement and the County may immediately terminate this Agreement for cause.
- (3) Contractor shall monitor the compliance of Contractor's personnel with the terms in Section 67 (Information Security Compliance), Exhibit C (Remote Access), and Exhibit E D(User Responsibility Statement for Third Parties), Exhibit E (FBI CJIS Security Addendum), Exhibit F (Executed CLETS Private Contractor Management Control Agreement), and Exhibit G (CLETS Employee/Volunteer Statement) and shall notify County no later than 24 hours after Contractor discovers any violations. Contractor's failure to monitor Contractor's employees or timely notify the County shall constitute a material breach of this Agreement, and the County may immediately terminate this Agreement for cause.

In the event of Immediate Termination for Cause, the rights and obligations in Section 19 (Termination for Cause) apply, except for the thirty (30) day notice period and ten (10) day cure period.

72. CLICK-THROUGH AGREEMENTS AND CONTRACTOR POLICIES

- (1) No provisions of any Contractor shrink-wrap or any click-through agreement (or other form of "click to accept" agreement) that may routinely accompany any products or services acquired under this Agreement shall apply in place of, or serve to modify any provision of this Agreement, to the extent that an authorized user of the County is acting in his/her scope of employment for the County even if such authorized user of County purports to have affirmatively accepted such shrink-wrap or click through provisions. Without limiting the foregoing, no "terms of use," "privacy policy" or other policy on Contractor's website or application (collectively, "Policies") or another website that may routinely accompany any products or services acquired under this Agreement shall apply in place of or serve to modify any provision of this Agreement to the extent that an authorized user of the County is acting in his/her scope of employment for the County.
- (2) For the avoidance of doubt and without limiting the foregoing, in the event of a conflict between any such Contractor shrink-wrap, click-through provisions or Policies (irrespective of the products or services that such provisions attach to) and any term or condition of this Agreement, the relevant term or condition of this Agreement shall govern to the extent of any such conflict. Only the provisions of this Agreement as amended from time to time, and executed by the parties, shall apply to County and or authorized user to the extent that the authorized user of the County is acting in his/her scope of employment for the County.
- (3) The parties acknowledge that the County and or authorized users may be required to click "Accept" as a routine condition of access to services through the Contractor's website or other application. Such Contractor click-through provisions or Policies on Contractor's website shall be null and void for County and/or each such authorized user solely to the extent that the authorized user of the County is acting in his/her scope of employment for the County and shall only serve as a mechanical means for accessing such services.
- (4) This provision shall not apply to the click-through provisions provided by other law enforcement agencies related to access to and use of their law enforcement data on a right-to-know, need-to-know basis.

73. FACIAL RECOGNITION TECHNOLOGY

Contractor shall not provide any facial recognition technology, including but not limited to FaceMatch, to the County, including its Office of the Sheriff, under this Agreement.

11. Replace Section 3(b) in **EXHIBIT B, FORENSIC LOGIC SUBSCRIPTION SERVICES AGREEMENT**, in its entirety with the following:

- b. **Data Restoration.** In the event of any loss or corruption of Customer Data, FL will use commercially reasonable efforts to restore the lost or corrupted Customer Data. FL shall not be responsible for any loss, destruction, alteration, unauthorized disclosure, or corruption of Customer Data caused solely by any third party. EXCEPT AS PROVIDED FOR IN EXHIBIT A (COUNTY OF SANTA CLARA TERMS AND CONDITIONS) AS AMENDED, FL' S EFFORTS TO RESTORE LOST OR CORRUPTED CUSTOMER DATA PURSUANT TO THIS SECTION SHALL CONSTITUTE FL' S SOLE LIABILITY AND CUSTOMER' S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF ANY LOSS OR CORRUPTION OF CUSTOMER DATA CAUSED SOLELY BY A THIRD PARTY. Customer acknowledges and agrees that FL will not be responsible for communications or Customer Data transmitted via the Subscription Services. Customer is solely responsible for the accuracy, quality, integrity, and legality of Customer Data.

12. Replace Section 6(a) in **EXHIBIT B, FORENSIC LOGIC SUBSCRIPTION SERVICES AGREEMENT**, in its entirety with the following:

- a. **Implementation Services.** FL will provide Implementation Services by assisting Customer and other SBISS agencies with configuration and integration of the Subscription Services with Customer's and other SBISS agencies' systems, including integration of County/SBISS Law Enforcement Data with the central data cache for the Forensic Logic Cloud. Customer and other SBISS agencies, and not FL, shall be solely responsible for obtaining, setting up, and maintaining, at Customer's or the SBISS agency's own expense, the servers, third party software, telecommunications and Internet services, and any other minimum system requirements specified by FL as necessary for proper installation, access, and use of the Subscription Services. Customer acknowledges that any warranty with respect to such third party hardware and/or software is provided exclusively by the manufacturer, and not by FL, and that FL shall have no obligation or liability whatsoever with respect to any such third party hardware and/or software.

13. Add Section 10(d), Exceptions, to **EXHIBIT B, FORENSIC LOGIC SUBSCRIPTION SERVICES AGREEMENT**, to read as follows:

- d. **Exceptions.** The limitations on liability in this Section 10 shall not apply to fraud, gross negligence, willful misconduct, the indemnity obligations in Exhibit A, or privacy or security breaches.

All other terms and conditions of the Agreement, as amended, remain in full force and effect. In the event of a conflict between the original Agreement, as amended, and this Amendment, this Amendment controls.

Contract Administered by: David Strausser, Strategic Sourcing Officer, at (408) 491-7447 or david.strausser@prc.sccgov.org

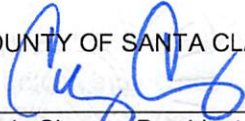
Prepared by: Sabrina Teixeira, Buyer II at (408) 491-7467 or Sabrina.Teixeira@prc.sccgov.org

The Agreement as amended, constitutes the entire agreement of the parties concerning the subject matter herein and supersedes all prior oral and written agreements, representations and understandings concerning such subject matter.

//

By signing below, signatory warrants and represents that he/she executed this Amendment in his/her authorized capacity, that he/she has the authority to bind the entity listed below to contractual obligations and that by his/her signature on this Amendment, the entity on behalf of which he/she acted, executed this Amendment.

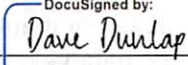
COUNTY OF SANTA CLARA


Cindy Chavez, President
Board of Supervisors

AUG 1 1 2020

Date

FORENSIC LOGIC, LLC

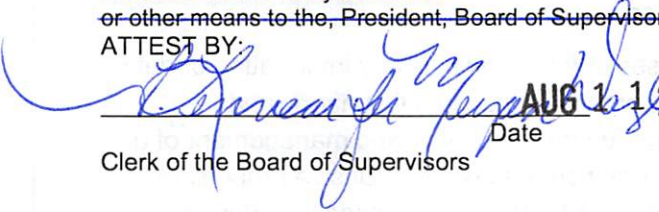
DocuSigned by:
By: 

Print: Dave Dunlap

Title: COO

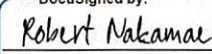
Date: 7/27/2020

~~Signed and certified that a copy of this document
has been delivered by electronic
or other means to the, President, Board of Supervisors~~
ATTEST BY:


AUG 1 1 2020
Date

Clerk of the Board of Supervisors

APPROVED AS TO FORM AND LEGALITY

DocuSigned by:

Robert Nakamae 7/28/2020
Date
Deputy County Counsel

Attachments:

- EXHIBIT C – REMOTE ACCESS
- EXHIBIT D – COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES
- EXHIBIT E – FBI CJIS SECURITY ADDENDUM
- EXHIBIT F – EXECUTED CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT
- EXHIBIT G – CLETS EMPLOYEE/VOLUNTEER STATEMENT
- APPENDIX 1.1 – PRICING SUMMARY

EXHIBIT C
REMOTE ACCESS

1. Definitions

- (a) "Remote Access" is the act of accessing County Systems from a non-County network infrastructure.
- (b) "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.
- (c) "County-owned information/data," for purposes of this Exhibit, is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.
- (d) "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

- (a) County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:

COPLINK Detect and LEAP Search Subscription

- (b) All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.
- (c) Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the Designated Systems
- (d) County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

- (a) Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets or exceeds NIST 800-53 standards, or an equivalent industry standard.
- (b) Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:
 - (i) Upon request by an authorized County representative, Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County reserves the right to advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.
 - (ii) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:
 - (aa) Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County-site-to-Contractor-site Virtual Private Network (VPN) infrastructure.
 - (bb) County personnel will control authorizations (permissions) to specific systems or networks.
 - (cc) All Contractor systems used to remotely access County Systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include the date, time, and user identification.

5. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County System unless otherwise stated in this Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in this Agreement.

6. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet or exceed NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

7. Remote Access Contacts

The following persons are points of contact for purposes of this Exhibit:

**Contractor: Nancy Keena, Account Manager
Forensic Logic, LLC**

712 Bancroft Road SPC 423
Walnut Creek, CA 94598
nkeena@forensiclogic.com

County: John Zore, Senior Systems Administrator
County of Santa Clara Office of the Sheriff
55 W. Younger Ave.
San Jose, CA 95110
john.zore@shf.sccgov.org

Either party may change the aforementioned names by providing the other party with no less than three (3) business days prior written notice.

8. Additional Requirements

Contractor agrees to the following:

- (a) Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.
- (b) Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
- (c) An encryption method that meets or exceeds Federal Information Processing Standard (FIPS) Publication 140-2 will be used.
- (d) Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall report any suspected security incident or concern to the County TechLink Center within 24 hours. The TechLink Center's contact information is (408) 918-7000, TLC@isd.sccgov.org.
- (e) Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.
- (f) Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.
- (g) Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees shall report loss or theft of such devices to the County TechLink Center within 24 hours. The TechLink Center's contact information is (408) 918-7000, TLC@isd.sccgov.org.

9. Remote Access Methods

- (a) All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County. The remote access solution must conform to County policy and security requirements.
- (b) Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

(c) Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is not applicable, please check the button marked N/A).

(i) **VPN Site-to-Site** **Primary** **Backup** **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the Contractor site and at the County, with a secure “tunnel” opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the Designated Systems from selected network-attached devices at the Contractor site.

(ii) **VPN Client Access** **Primary** **Backup** **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

An Authentication Token (a physical device or software token that an authorized remote access user is given for user authentication purposes, such as a CryptoCard, RSA token, SecureAuth IdP, Arcot software token, or other such one-time-password mechanism approved by the County Information Security Office) will be issued to the Contractor in order to authenticate Contractor staff when accessing County Designated Systems via this method. The Contractor agrees to the following when issued an Authentication Token:

- a. Because the Authentication Token allows access to privileged or confidential information residing on the County’s Designated Systems, the Contractor agrees to treat the Authentication Token as it would a signature authorizing a financial commitment on the part of the Contractor.
- b. A hardware Authentication Token is a County-owned physical device, and will be labeled as such. The label must remain attached at all times.
- c. The Authentication Token is issued to an individual employee of the Contractor and may only be used by the designated individual.
- d. The Authentication Token must be kept in the possession of the individual Contractor employee it was issued to or in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.
- e. If the Contractor’s remote access equipment is moved to a non-secured site, such as a repair location, the Authentication Token will be kept under Contractor control.
- f. If the Authentication Token is misplaced, stolen, or damaged, the Contractor will notify the County TechLink Center by phone within 24 hours.
- g. Contractor agrees to use the Authentication Token as part of its normal business operations and for legitimate business purposes only.
- h. The Authentication Token will be issued to Contractor following execution of this Agreement. Hardware Authentication Tokens will be returned to the County’s Tech Link Center within five (5) business days following contract termination, or upon written request of the County for any reason.
- i. Contractor will notify the County’s the County TechLink Center within one working day of any change in personnel affecting use and possession of the

Authentication Token. The TechLink Center's contact information is (408) 918-7000, TLC@isd.sccgov.org. Contractor will obtain the Authentication Token from any employee who no longer has a legitimate need to possess the Authentication Token. The County will recoup the cost of any lost or non-returned hardware Authentication.

- j. Contractor will not store account or password documentation or PINs with Authentication Tokens.
- k. Contractor will ensure all Contractor employees that are issued an Authentication Token will be made aware of and provided with a written copy of the requirements set forth in this Exhibit.

(iii) County-Controlled VPN Client Access Primary Backup N/A

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the Authentication Token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes. When the Contractor needs to access County Designated Systems, the Contractor must first notify the County's Remote Access Contact.

The County's TechLink Center will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's Designated Systems. Contractor agrees to the following:

- a. Because the PIN number allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.
- b. The PIN number is confidential, County-owned, and will be identified as such.
- c. The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.
- d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.
- e. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.
- f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.
- g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to Designated Systems, other County Systems, and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
- h. The PIN number will be issued to Contractor following execution of this Agreement.
- i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

(iii) **County-Controlled Enexity Access** **Primary** **Backup** **N/A**

The County-Controlled Enexity Access method involves using Securelink's Enexity tool installed in the County. County will establish a gateway where Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through Enexity gateways.

Signatures of Contractor Employees receiving Authentication Tokens (**Only for VPN Client Access and if tokens issued by County**):

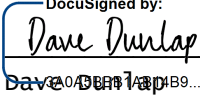
SIGNATURE:  _____
Date: 7/27/2020

EXHIBIT D
COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT
FOR THIRD PARTIES

1. DEFINITIONS

- (a) “*County Confidential Information*” is all material non-public information, written or oral, disclosed, directly or indirectly, through any means of communication or observation by County to Contractor or any of its affiliates or representatives
- (b) “*County Systems*” include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. “*County Systems*” also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.
- (c) “*County-owned information/data,*” for purposes of this Exhibit is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User’s personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.
- (d) “*Mobile Device*” is any portable computing device that fits one of the following categories: laptops, smartphones, or tablets. “*Mobile Device*” does not include devices that are used exclusively for the purpose of making telephone calls.
- (e) “*Users*” include all employees, agents and/or representatives of Contractor performing services under this Agreement.

2. GENERAL REQUIREMENTS

- (a) Contractor will provide Users with a written copy of this Exhibit and will ensure that Users know, understand and comply with the requirements of this Exhibit. Users allowed access to County resources shall sign the Acknowledgement and Receipt. In all cases, such access shall be subject to approval by an authorized County representative.
- (b) Users are personally responsible for knowing and understanding these requirements, and are personally responsible for any actions they take that do not comply with County policies and standards. If a User is unclear as to requirements, User shall ask County for guidance.
- (c) If a User is issued an account for a County System, User shall comply with the following County standards for password definition, use, and management:
 - (i) Minimum password length is 12 characters unless a particular County System has a different requirement or is not technically feasible.

- (ii) The password must be high complexity (contains one of each, upper, lower, number, symbol).
 - (iii) The password must be rotated every 90 days.
 - (iv) User must not reuse the last 10 passwords.
 - (v) Access to County System is denied after 5 failed logon attempts.
- (d) Only authorized County staff may attach any form of computer equipment to a County network or system. This includes, but is not limited to, attachment of such devices as mobile devices, peripherals (e.g., external hard drives, printers), and USB storage media. It excludes County wireless networks provided specifically for the use of guests or visitors to County facilities.
- (e) User shall not use USB storage media on any County System. All such devices shall be County-owned, formally issued to User by County, and used only for legitimate County purposes.
- (f) User shall not connect County-owned computing equipment, including USB storage media, to non-County systems or networks, unless County gives its express written permission. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home network.
- (g) User shall not install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County System, without County's express written permission. If authorized to install, configure or use such a device, User shall comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County Systems. Any allowed installation shall not be activated until it is reviewed and approved in writing by an authorized County representative.
- (h) The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.
- (i) Users shall not attempt to elevate or enhance their assigned level of privileges unless County gives its express written permission. Users who have been granted enhanced privileges due to their specific roles, such as system or network administrators, shall not abuse these privileges and shall use such privileges only in the performance of appropriate, services performed under this Agreement.
- (j) Users shall use County-approved authentication mechanisms when accessing County networks and systems, and shall not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by County.
- (k) Users shall not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or installed, it is the responsibility of the User to check with County.
- (l) All software on County Systems shall be installed by authorized County support staff except as provided in this Agreement. Users may not download or install software on any County system unless express written permission has been obtained from County such as in this Agreement.

- (m) Users shall immediately report to the County TechLink Center the loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business or performing services under a Supplemental Agreement. The TechLink Center's contact information is (408) 918-7000, TLC@isd.sccgov.org.
- (n) Users must be aware of security issues and shall immediately report incidents to the County Information Security Office involving breaches of the security of County Systems or breaches of County-owned information/data, such as the installation of an unauthorized device, or a suspected software virus or other occurrences of malicious software or content. The Information Security Office's contact information is o365-iso-team@sccconnect.onmicrosoft.com.
- (o) Users shall respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:
 - (i) Users shall not access, or attempt to access, County Systems or County-owned information/data unless specifically authorized to do so by the terms of this Agreement.
 - (ii) If User is assigned a County account, User shall not allow unauthorized individuals to use their account; this includes the sharing of account passwords.
 - (iii) Users shall not without County's written permission, use or disclose County-owned information/data other than in the performance of its obligations under this Agreement.
 - (iv) Users shall take every precaution to ensure that all confidential or restricted information is protected from disclosure to unauthorized individuals.
 - (v) Users shall not make or store paper or electronic copies of information unless required to provide services under this Agreement.
 - (vi) Users shall comply with all confidentiality requirements in Contractor's Agreement with the County. Users shall not use or disclose County Confidential Information other than in the performance of its obligations for County. All County Confidential Information shall remain the property of the County. User shall not acquire any ownership interest in County Confidential Information.
- (p) Users shall do all of the following:
 - (i) Users shall not change or delete County-owned information/data unless performing such changes is required to perform services under this Agreement.
 - (ii) Users shall avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.
 - (iii) Upon termination or expiration of this Agreement, Users shall not retain, give away, or remove any County-owned information/data or document from any County System or County premises. Users shall return to County all County-owned assets, including hardware and data.
- (q) Electronic information transported across any County network, or residing in any County System, is potentially subject to access by County technical support staff, other County personnel, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County System.
- (r) Users must protect, respect and not infringe upon all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, County Confidential Information, and confidential information belonging to any other third party.

- (s) All information resources on any County System are the property of County and are therefore subject to County policies regarding acceptable use. No User may use any County System or County-owned information/data for the following purposes:
- (i) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization that are not related to the User conducting County business. This prohibition does not apply to User's performance of contractual obligations for the County.
 - (ii) Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.
 - (iii) To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business.
 - (iv) To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business.
 - (v) Knowingly propagating or downloading viruses or other malicious software.
 - (vi) Disseminating hoaxes, chain letters, or advertisements.

3. INTERNET AND EMAIL

- (a) Users shall not use County Systems for personal activities.
- (b) When conducting County business or performing services under this Agreement, Users shall not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by County. Such services include, but are not limited to, file sharing (such as Dropbox, Box, Google OneDrive), Instant Messaging (such as AOL IM), email services (such as Hotmail and Gmail), peer-to-peer networking services (such as Kazaa), and social networking services (such as blogs, Instagram, Snapchat, MySpace, Facebook and Twitter). If a User has received express written permission to access such services, User shall comply with all relevant County policies, procedures, and guidelines.
- (c) Users assigned a County email account must comply with the County's Records Retention and Destruction Policy.
- (d) Users shall not use an internal County email account assigned to another individual to either send or receive email messages.
- (e) Users shall not configure a County email account so that it automatically forwards messages to an external Internet email system unless County gives its express written permission.

4. REMOTE ACCESS

- (a) Users are not permitted to implement, configure, or use any remote access mechanism unless the County has authorized the remote access mechanism.
- (b) County may monitor and/or record remote access sessions, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County

may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

- (c) User shall configure all computer devices used to access County resources from a remote location according to NIST 800-53 standards, or an equivalent industry standard. These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by County.
- (d) Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Users shall immediately report loss or theft of such devices to the County TechLink Center at (408) 918-7000, TLC@isd.sccgov.org.
- (e) Users shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall immediately report any suspected security incident or concern to the County Information Security Office at o365-iso-team@sccconnect.onmicrosoft.com.
- (f) Users shall comply with any additional remote access requirements in this Agreement such as an Exhibit on Remote Access.

5. THIRD PARTY-OWNED DEVICES

- (a) This Section 5 applies if County permits Users to perform services under this Agreement with devices not owned by the County (“Third-party owned device”). Third-party owned devices include devices with email and/or data storage capability (such as laptops, iPhones, iPads, Android phones and tablets, BlackBerry and other “smart” devices).
- (b) The third party-owned device in question shall use existing, County-approved and County-owned access/authentication systems when accessing County Systems.
- (c) Users shall allow County to configure third party-owned devices as appropriate to meet security requirements, including the installation of specific security software mandated by County policy.
- (d) Use of a third party-owned device shall comply with County policies and procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule on at least a monthly basis. County may verify software installations and updates.
- (e) Users have no expectation of privacy with respect to any County-owned communications, information, or files on any third party-owned device. User agrees that, upon request, the County may immediately access any and all work-related or County-owned information/ data stored on these devices, in order to ensure compliance with County policies.
- (f) Users shall adhere to all relevant County security policies and standards, just as if the third party-owned device were County property. This includes, but is not limited to, policies regarding password construction and management, physical security of the device, device configuration including full storage encryption, and hard drive and/or storage sanitization prior to disposal.
- (g) Users shall not make modifications of any kind to operating system configurations implemented by County on the device for security purposes, or to any hardware or software installed on the device by County.
- (h) Users shall treat the contract-related or County-owned communications, information or files the third-party owned device contains as County property. User shall not allow

access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by County to access or use that data.

- (i) Users shall report immediately to the County Information Security Office o365-iso-team@sccconnect.onmicrosoft.com, any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the third-party owned device, and shall report immediately to the Tech Link Center at (408) 918-7000, TLC@isd.sccgov.org, the loss or theft of the device.

6. ACKNOWLEDGEMENT AND RECEIPT


This Acknowledgement hereby incorporates the URS.

By signing below, I acknowledge that I have read and understand all sections of this URS. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of my relationship with County and/or criminal prosecution.

Have you been granted Remote Access Yes No

I have read and understand the contents of the URS regarding Remote Access and the Exhibit on Remote Access. I understand that violation of these provisions may result in disciplinary action, up to and including termination of my relationship with the County and/or criminal prosecution. I received approval from County for remote access for legitimate County business, as evidenced by the signatures below.

User Signature:

DocuSigned by:

3A0A5BBB1AB14B9...

Date Signed:

7/27/2020

Print User Name:

Dave Dunlap

**APPENDIX 1.1
PRICING SUMMARY**

Term: June 1, 2020 through November 30, 2020. (6 Months)

Product	Quantity	List Price	Sales Price	Price
COPLINK Detect and LEAP Search Subscription Term: 6/1/2020 – 11/30/2020 COPLINK Detect and LEAP Search Subscription includes: Visualizer, Map Analyzer, Computer Statistics, Adaptive Analytic Architecture (A3), Active Agent, FaceMatch*, SRMA, Analysis Search (1 User), Inbound/Outbound Connectors for LEXS-SR, File Exporter for COPLINK IEPD and LEAP Search	3403	\$299.00	\$92.57	\$157,507.86
COPLINK LEAP Search Data Protect: Term: 6/1/2020 – 11/30/2020	1	\$5,250.00	N/A	\$5,250.00
COPLINK LEAP Vendor Data Integration/Re-Integrations: <ul style="list-style-type: none"> • Monterey Co SO – JMS • San Benito Co SO – JMS Term 6/1/2020 – 11/30/2020	1	\$15,500.00	N/A	\$15,500.00
Total Price				\$178,257.86

* Contractor shall not provide any facial recognition technology, including but not limited to FaceMatch, to the County, including its Office of the Sheriff, under this Agreement.



CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Agreement to allow California Law Enforcement Telecommunications System (CLETS) access by

Santa Clara County Office of the Sheriff and attached list of Agencies

(Public law enforcement/criminal justice agency)

CA0430000

(ORI)

to Forensic Logic

(Private Contractor)

to perform COPLINK and LEAP software updates and maintenance services on its behalf.

(Type of service)

Access to the CLETS is authorized to public law enforcement and criminal justice agencies (*hereinafter referred to as the CLETS subscribing agency*) only, which may delegate the responsibility of performing the administration of criminal justice functions (e.g., dispatching functions or data processing/information services) in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Addendum to a private contractor. The private contractor may access systems or networks that access the CLETS on behalf of the CLETS subscribing agency to accomplish the above-specified service(s). This agreement must be received by the California Department of Justice (CA DOJ) prior to the subscribing agency permitting access to the CLETS. The performance of such delegated services does not convert that agency into a public criminal justice agency, not automatically authorize access to state summary criminal history information. Information from the CLETS is confidential and may be used only for the purpose(s) for which it is authorized. Violation of confidentiality requirements or access authorizations may be subject to disciplinary action or criminal charges.

Pursuant to the policies outlined in the *CLETS Policies, Practices, and Procedures (PPP)* and the Federal Bureau of Investigation's (FBI) *CJIS Security Policy*, it is agreed the CLETS subscribing agency will maintain responsibility for security control as it relates to the CLETS access. Security control is defined as the ability of the CLETS subscribing agency to set, maintain, and enforce:

1. Standards for the selection, supervision, and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant CLETS access to personnel who meet these standards and deny it to those who do not.
2. Policies governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CA DOJ criminal justice databases used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Security control includes, but is not limited to, the supervision of applicable equipment, systems design, programming, and operating procedures associated with the development, implementation, and operation of any computerized message-switching or database systems utilized by the served law enforcement agency or agencies. Computer sites must have adequate physical security to protect against any unauthorized viewing or access to computer terminal, access devices, or stored/printed data.



CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all private contractors receiving information from the CLETS meet the minimum training, certification, and background requirements that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing information from the CLETS. The minimum requirements include, but are not limited to:

1. Prior to allowing the CLETS access, train, functionally test, and affirm the proficiency of all the CLETS computer operators to ensure compliance with the CLETS and the FBI's National Crime Information Center (NCIC) policies and regulations, if applicable. Biennially, provide testing and reaffirm the proficiency of all the CLETS operators, if applicable.
2. State and FBI criminal offender record information searches must be conducted prior to allowing access to the CLETS computers, equipment, or information. If the results of the criminal offender record information search reveal a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.
3. Each individual must sign a CLETS Employee/Volunteer Statement form (HDC 0009) prior to operating or having access to CLETS computers, equipment, or information.

In accordance with CLETS/NCIC policies, the CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the private contractor. The private contractor agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement and to accomplish the directives for service under the provisions of this agreement. The CLETS Management Control Agreement (HDC 0004B) shall be updated when the head of either agency changes or immediately upon request from the CA DOJ.

By signing this agreement, the vendors and private contractors certify they have read and are familiar with the contents of (1) the FBI's CJIS Security Addendum, (2) the NCIC 2000 Operating Manual, (3) the FBI's CJIS Security Policy, (4) Title 28, Code of Federal Regulations, Part 20, and (5) the CLETS PPP and agree to be bound by their provisions. Criminal offender record information and related data, by its very nature, is sensitive and has potential for great harm if misused. Access to criminal offender record information and related data is therefore limited to the purpose(s) for which the CLETS subscribing agency has entered into the contract. Misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; use, dissemination, or secondary dissemination of 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. Accessing the system for an appropriate purpose and then using, disseminating, or secondary dissemination of information received for another purpose other than execution of the contract also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.



 Signature (CLETS Subscribing Agency Head)



 Signature (Private Contractor Agency Head)

Laurie Smith, Sheriff

 Print Name and Title

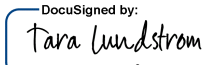
Robert L Batty, Executive Chairman

 Print Name and Title

APPROVED AS TO FORM AND LEGALITY

7-19-18

 Date

DocuSigned by:

 Tara Lundstrom

 Deputy County Counsel

01/18/2018

 Date

Additional Agencies covered by the MCA with Forensic Logic.

Campbell PD
Foothill – De Anza Community College PD
Gilroy PD
Los Altos PD
Los Gatos PD
Milpitas PD
Morgan Hill PD
Mountain View PD
Palo Alto PD
San Jose PD
San Jose City College/Evergreen Community College PD
San Jose State University PD
Santa Clara PD
Santa Clara County Office of the District Attorney
Santa Clara County Probation
Sunnyvale DPS
Capitola PD
Santa Cruz PD
Santa Cruz County District Attorney
Santa Cruz County Probation
Santa Cruz County Sheriff
Scotts Valley PD
Watsonville PD
Carmel PD
California State University Monterey Bay PD
Del Rey Oaks PD
Gonzales PD
Greenfield PD
King City PD
Marina PD
Monterey PD
Monterey County District Attorney
Monterey County Probation
Monterey County Sheriff's Office
Pacific Grove PD
Salinas PD
Sand City PD
Seaside PD
Soledad PD
Hollister PD
San Benito County District Attorney
San Benito County Probation
San Benito County Sheriff's Office

EXHIBIT F

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.

1.1 Definitions

1.2 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.

1.3 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.

2.1 Responsibilities of the Contracting Government Agency.

2.2 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).

3.1 Responsibilities of the Contractor.

3.2 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).

4.1 Security Violations.

- 4.2 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.
- 4.3 Security violations can justify termination of the appended agreement.
- 4.4 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.
- 5.1 Audit
- 5.2 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.
- 6.1 Scope and Authority
- 6.2 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.
- 6.3 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.
- 6.4 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.
- 6.5 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.
- 6.6 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

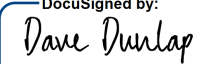
Clarksburg, West Virginia 26306

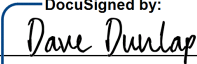
**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

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.

Dave Dunlap	<small>DocuSigned by:</small>  <small>3A0A5BBB1AB14B9...</small>	7/27/2020
Printed Name/Signature of Contractor Employee		Date

Dave Dunlap	<small>DocuSigned by:</small>  <small>3A0A5BBB1AB14B9...</small>	7/27/2020
Printed Name/Signature of Contractor Representative		Date

Forensic Logic, LLC COO

Organization and Title of Contractor Representative



CLETS EMPLOYEE/VOLUNTEER STATEMENT

Print Form

Use of information from the California Law Enforcement Telecommunications System (CLETS) and the Department of Motor Vehicles record information

As an employee/volunteer of Forensic Logic, LLC, you may have access to confidential criminal records, the Department of Motor Vehicle (DMV) records or other criminal justice information, much of which is controlled by statute. All information from the CLETS is based on the "need-to-know" and the "right-to-know" basis. Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644. The misuse of such information may adversely affect an individual's civil rights and violates the law and/or CLETS policies.

Penal Code (PC) section 502 prescribes the penalties relating to computer crimes. PC sections 11105 and 13300 identify who has access to state and local summary criminal history information and under which circumstances it may be released. PC sections 11141–11143 and 13302–13304 prescribe penalties for misuse of state and local summary criminal history information. Government Code section 6200 prescribes the felony penalties for misuse of public records and information from the CLETS. California Vehicle Code section 1808.45 prescribes the penalties relating to misuse of the DMV record information.

PC sections 11142 and 13303 state:

"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."

Any employee/volunteer who is responsible for the CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL INFORMATION FROM THE CLETS.

DocuSigned by:
Dave Dunlap
Signature

Dave Dunlap

Print Name

7/27/2020

Date