County of Santa Clara
Office of the County Executive
Procurement Department
150 West Tasman Dr., First Floor
San Jose, CA 95134
Telephone 408-491-7400 • Fax 408-491-7496

AGREEMENT BETWEEN THE COUNTY OF SANTA CLARA AND IDEMIA IDENTITY & SECURITY USA LLC.

This Agreement is entered into between the County of Santa Clara ("County") and Idemia Identity & Security USA LLC ("Contractor") to provide Automated Fingerprint Identification System (AFIS) including AFIS Disaster Recovery and Live Scan maintenance and support.

Now therefore in consideration of the mutual covenants contained in this Agreement, the parties mutually agree as follows:

KEY PROVISIONS

AGREEMENT TITLE	AFIS, AFIS Disaster Recovery, and LiveScan Maintenance and Support
AGREEMENT NUMBER	CW2233126
AGREEMENT TERM	October 1, 2019 through June 30, 2024 unless terminated earlier or otherwise amended.
TOTAL AGREEMENT VALUE	$2,460,000 *Contractor understands that this is a not to exceed value and does not represent a commitment by County to Contractor.*
PAYMENT TERMS	Net 45
COMMODITY NAME / CODE	Hardware Maintenance and Support Services / 45000
PURPOSE	To provide annual maintenance and support services for Automated Fingerprint Identification System (AFIS) including AFIS Disaster Recovery System and LiveScan
AUTHORIZED USER	Sheriff's Office (SHO) 55 West Younger Ave. San Jose, CA 95110

COUNTY DEPARTMENT CONTACT	Tim Fayle, Fingerprint Identification Director Sheriff's Identification Unit (SIU) Sheriff's Office 55 West Younger Ave. San Jose, CA 95110 Phone: 408-808-4744 Email: timothy.fayle@shf.sccgov.org
COUNTY CONTRACT ADMINISTRATOR	Martin Coronel, Procurement Contracts Specialist Phone: (408) 491-7467 Email : martin.coronel@prc.sccgov.org Minh-Thao Nguyen, Buyer II Phone: (408) 491-7405 Email : minh-thao.nguyen@prc.sccgov.org
CONTRACTOR	Idemia Identity & Security USA LLC 11951 Freedom Drive, Suite 1800 Reston, VA 20190
CONTRACTOR CONTACT	Gordon Warden, Region Service Manager Phone : (936) 570-9427 Email : gordon.warden@idemia.com
CONTRACTOR NUMBER	1034871
TAX STATUS	Non-Taxable

EXHIBITS

Contractor shall comply with the exhibits to this Agreement, which are attached hereto and incorporated into this Agreement by reference. In the event of any conflict between or among the provisions contained in the Agreement, the order of precedence is as follows:

Exhibit A – County of Santa Clara Standard Terms and Conditions

Exhibit B – Maintenance Fees Schedule

Exhibit C – Insurance Requirements

Exhibit D – County Security Addendum

Exhibit E – County Information Technology User Responsibility Statement for Third Parties

Exhibit F – Vendor Remote Access Agreement

Exhibit G – Private Contractor Management Control Agreement

Exhibit G-1 – CLETS Employee/Volunteer Statement

Exhibit H – FBI CJIS Security Addendum

Exhibit I – Idemia License Agreements
Exhibit I-1: Biometric Products and System Sales Agreement
Exhibit I-2: Software License Agreement

By signing below, signatory warrants and represents that he/she executed this Agreement 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 Agreement, the entity on behalf of which he/she acted, executed this Agreement.

COUNTY OF SANTA CLARA

DocuSigned by:
Caroline Kho
2B8B2DFCD8084D2...
9/5/2019
Caroline Kho Date
Strategic Sourcing Manager

Alice C. Bailey 9/26/2019
Alice C. Bailey Date
Director of Procurement

CONTRACTOR

9/18/2019
Michael Kato Date
Vice President

APPROVED AS TO FORM AND LEGALITY

DocuSigned by:
Robert Nakamae
797E74E07E8345C...
9/5/2019
Robert Nakamae Date
Deputy County Counsel

EXHIBIT A
COUNTY OF SANTA CLARA STANDARD TERMS AND CONDITIONS

DEFINITIONS

a. "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.
b. "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.
c. "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.
d. "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.
e. When used in this Agreement, "days" shall refer to calendar days unless stated otherwise.
f. "Breach" means unauthorized access to, or use of, County Data or information security networks or systems that compromises confidentiality, integrity, and/or availability those systems or County Data.
g. "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.
h. "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 (ii) the potential impact on the County of any security risks, weaknesses and threats related to safeguarding County assets and County Data. The Risk Assessment usually includes the ISO's evaluation of documentation provided by the Contractor.

1. NON-EXCLUSIVE AGREEMENT

The Agreement does not establish an exclusive contract between the County and the Contractor. The County expressly reserves rights to, without limitation, the following: the right to utilize others to provide products, support and services; the right to request proposals from others with or without requesting proposals from the Contractor; and the unrestricted right to bid any such product, support or service.

2. DELIVERABLES

Contractor agrees to provide the County all Deliverables on terms set forth in the Agreement, including all Exhibits that are attached to the Agreement and incorporated, as well as all necessary equipment and resources. However, this Agreement does not provide authority to ship Deliverables. That authority shall be established by contract release purchase orders placed by the County and sent to Contractor throughout the term of the Agreement. Each and every contract release purchase order shall incorporate all terms of this Agreement and this Agreement shall apply to same.

Any additional or different terms or qualifications sent by Contractor, including, without limitation,

electronically or in mailings, attached to invoices or with any deliverables shipped, shall not become part of the contract between the parties. County's acceptance of Contractor's offer is expressly made conditional on this statement.

Contractor shall timely provide to the County, all documentation and manuals relevant to the Deliverables to be supplied, at no additional cost. Such documentation shall be delivered either in advance of the delivery of Deliverables or concurrently with the delivery of Deliverables.

Employees and agents of Contractor, shall, while on the premises of the County, comply with all rules and regulations of the premises, including, but not limited to, security requirements. If required, Contractor shall be responsible for installation, training and knowledge transfer activities in relation to the Deliverables being supplied.

All equipment shall be delivered to a County site specified in the contract release purchase order, or if not so specified therein, in the Statement of Work/Specifications.

Contractor holds itself out as an expert in the subject matter of the Agreement. Contractor represents itself as being possessed of greater knowledge and skill in this area than the average person. Accordingly, Contractor is under a duty to exercise a skill greater than that of an ordinary person, and the manner in which performance is rendered will be evaluated in light of the Contractor's superior skill. Contractor shall provide equipment and perform work in a professional manner consistent, at minimum, with industry standards.

Contractor represents that all prices, warranties, benefits and other terms being provided hereunder are fair, reasonable and commensurate with the terms otherwise being offered by Contractor to its current customers ordering comparable Deliverables and services. County does not guarantee any minimum orders.

3. NECESSARY ACTS AND FURTHER ASSURANCES

The Contractor shall at its own cost and expense execute and deliver such further documents and instruments and shall take such other actions as may be reasonably required or appropriate to evidence or carry out the intent and purposes of this Agreement.

4. COUNTING DAYS

Days are to be counted by excluding the first day and including the last day, unless the last day is a Saturday, a Sunday, or a legal holiday, and then it is to be excluded.

5. PRICING

The Contract Price is in U.S. Dollars.

Unless otherwise stated, prices shall be fixed for the term of the Agreement, including all extensions. If any product listed in this Agreement is discontinued or upgraded prior to delivery, Contractor shall extend the same pricing towards a comparable replacement which is functionally equivalent or an upgraded version.

Exhibit B of the Agreement is the basis for pricing and compensation throughout the term of the Agreement.

Notwithstanding the above, if at any time during the term of the Agreement the Contractor offers special, promotional or reduced pricing when compared with the price paid by the County, County shall benefit from that pricing, and that pricing shall apply to the County at the same time that is offered to other entities. Contractor is required, on an ongoing basis, to inform the County of any such special, promotional or reduced pricing.

6. MODIFICATION
This Agreement or any contract release purchase order may be supplemented, amended, or modified only by the mutual agreement of the parties. No supplement, amendment, or modification of this Agreement contract release purchase order will be binding on County unless it is in writing and signed by the County's authorized representative.

7. TIME OF THE ESSENCE
Time is of the essence in the delivery of goods by Contractor under this Agreement and any contract release purchase order. If Contractor fails to deliver goods and/or services on time, the Contractor shall be liable for any costs incurred by the County because of Contractor's delay. For instance, County may purchase or obtain the goods and/or services elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County; or County may terminate on grounds of material and Contractor shall be liable for County's damages.

The Contractor shall promptly reimburse the County for the full amount of its liability, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

8. HAZARDOUS SUBSTANCES
If any product being offered, delivered or supplied to the County is listed in the Hazardous Substances List of the Regulations of the Director of Industrial Relations with the California Occupational Safety and Health Standards Board, or if the product presents a physical or health hazard as defined in the California Code of Regulations, General Industry Safety Order, Section 5194 (T8CCR), Hazard Communication, the Contractor must include a Material Safety Data Sheet (MSDS) with delivery, or shipment. Each MSDS must reference the contract/purchase order number, and identify the "Ship To Address". All shipments and containers must comply with the labeling requirements of Title 49, Code of Federal Regulations by identifying the hazardous substance, name and address of manufacturer, and appropriate hazard warning regarding potential physical safety and health hazard.

9. SHIPPING AND RISK OF LOSS
Goods shall be packaged, marked and otherwise prepared by Contractor in suitable containers in accordance with sound commercial practices. Contractor shall include an itemized packing list with each shipment and with each individual box or package shipped to the County. The packing list shall contain, without limitation, the applicable contract release purchase order number.

Unless otherwise specified in writing, all shipments by Contractor to County will be F.O.B. point of destination. Freight or handling charges are not billable unless such charges are referenced on the order. Transportation receipts, if required by contract release purchase order, must accompany invoice. Regardless of F.O.B. point, Contractor agrees to bear all risks of loss, injury, or destruction to goods and materials ordered herein which occur prior to delivery at County's destination; and such loss, injury or destruction shall not release Contractor from any obligation hereunder.

Any shipments returned to the Contractor shall be delivered as F.O.B. shipping point.

10. INSPECTION AND RELATED RIGHTS
All goods and services are subject to inspection, testing, approval and acceptance by the County.

Inspection shall be made within 60 days or a reasonable time after delivery, whichever period is longer. If the goods, services, or the tender of delivery fail in any respect to conform to the contract, the County may reject the entire tender, accept the entire tender, or, if the deliverables are commercially divisible, may, at its option, accept any commercial unit or units and reject the rest.

Contractor shall be responsible to reclaim and remove any rejected goods or items at its own expense. Should Contractor fail to reclaim or remove any rejected goods or items within a reasonable time, County shall, at its option dispose of such goods or items and require reimbursement from Contractor for any costs or expenses incurred.

In the event that the Contractor's goods are not accepted by County, the Contractor shall be liable for any costs incurred by the County because of such failure by Contractor. For instance, County may purchase or obtain the goods elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County, and any other costs incurred; or County may terminate for cause on grounds of material breach and Contractor shall be liable for County's damages.

The Contractor shall promptly reimburse the County for the full amount of its liability, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

11. ADJUSTMENT BY COUNTY

The County reserves the right to waive a variation in specification of goods or services supplied by the Contractor. Contractor may request an equitable adjustment of payments to be made by County if County requires a change in the goods or services to be delivered. Any claim by the Contractor for resulting adjustment of payment must be asserted within 30 days from the date of receipt by the Contractor of the notification of change required by County; provided however, that the County's authorized representative decides that the facts justify such action, may receive and act upon any such claim asserted at any time prior to final payment made for goods and services supplied by Contractor. Where the cost of property made obsolete or excess as a result of a change is included in the Contractor's claim for adjustment, the County's authorized representative shall have the right to prescribe the manner of disposition of such property. Nothing in this clause shall excuse performance by Contractor.

12. INVOICING

Contractor shall invoice according to Exhibit B of the Agreement. Invoices shall be sent to the County customer or department referenced in the individual contract release purchase order. Invoices for goods or services not specifically listed in the Agreement will not be approved for payment.
Invoices shall include: Contractor's complete name and remit-to address; invoice date, invoice number, and payment term; County contract number; pricing per the Agreement; applicable taxes; and total cost.
Contractor and County shall make reasonable efforts to resolve all invoicing disputes within seven (7) days.

13. PAYMENT

The County's standard payment term shall be Net forty-five (45), unless otherwise agreed to by the parties. Payment shall be due Net forty-five (45) days from the date of receipt and approval of correct

and proper invoices.
Notwithstanding the standard payment term set forth above, the parties agree that the Payment Term for this Agreement shall be the term set forth in the Key Provisions section of the Agreement above. If the Payment Term is a prompt payment discount term, then payment shall be made accordingly. For example, if the Payment Term is 2.25% ten (10) Net forty-five (45), payment shall be due ten (10) days from the date the County receives and approves the correct and proper invoice, but no later than forty-five (45) days from that date, and the County would take a discount of 2.25% of the total amount of the invoice if the payment is made in ten (10) days. The parties also agree that notwithstanding the Payment Term set forth in the Key Provisions section of the Agreement, that at any time during the contract term, either party may initiate an early payment discount on an invoice-by-invoice basis utilizing the Dynamic Discounting functionality of the Ariba Network. Contractor must have a registered account on the Ariba Network to utilize this functionality.
Payment is deemed to have been made on the date the County mails the warrant or initiates the electronic fund transfer.

14. OTHER PAYMENT PROVISIONS
Notwithstanding anything to the contrary, County shall not make payments prior to receipt of service or goods (i.e. the County will not make "advance payments"). Unless specified in writing in an individual purchase order, the County will not accept partial delivery with respect to any purchase order. Any acceptance of partial delivery shall not waive any of County's rights on an ongoing basis.

Sales tax shall be noted separately on every invoice. Items that are not subject to sales tax shall be clearly identified.

Contractor shall be responsible for payment of all state and federal taxes assessed on the compensation received under this Purchase Order and such payment shall be identified under the Contractor's federal and state identification number(s).

The County does not pay Federal Excise Taxes (F.E.T). The County will furnish an exemption certificate in lieu of paying F.E.T. Federal registration for such transactions is: County #94730482K. Contractor shall not charge County for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose, unless expressly authorized by the County.

15. LATE PAYMENT CHARGES OR FEES
The Contractor acknowledges and agrees that the County will not pay late payment charges.

16. DISALLOWANCE
In the event the Contractor receives payment for goods or services, which payment is later disallowed by the County or state or federal law or regulation, the Contractor shall promptly refund the disallowed amount to the County upon notification. At County's option, the County may offset the amount disallowed from any payment due to the Contractor under any contract with the County.

17. TERMINATION FOR CONVENIENCE
The County may terminate this Agreement or any order at any time for the convenience of the County, specifying the effective date and scope of such termination.
In no event shall the County be liable for costs incurred by the Contractor as a result of the termination or any loss of profits on the resulting order or portion thereof so terminated. In the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other materials (collectively referred to as "materials") prepared by Contractor under this Agreement contract release purchase order shall become the property of the County and shall be promptly delivered to the County. Upon receipt of such materials, County shall pay the Contractor as full compensation for performance, the unit or pro rata price for the then-accepted portion of goods and/or services. If this Agreement is terminated, neither party may nullify obligations, if any, already

incurred prior to the date of termination.

Termination for Convenience may be exercised anytime by and at the sole discretion of the County.

18. TERMINATION FOR CAUSE

Default by a Party. Either Party may terminate this Agreement or any order, in whole or in part, for cause upon thirty (30) days written notice to the other Party (unless a Force Majeure causes the default). For purposes of this Agreement, cause includes, but is not limited to, any of the following: (a) material breach of this Agreement or any contract release purchase order by the other Party, (b) violation by the other Party of any applicable laws or regulations; (c) assignment or delegation by Contractor of the rights or duties under this Agreement without the written consent of County, (d) less than perfect tender of delivery or performance by Contractor that is not in strict conformance with terms, conditions, specifications, covenants, representations, warranties or requirements in this Agreement or any order, or (d) default by the County for failing to pay any amount due under this Agreement.

In the event County terminates for cause under this provision, the Contractor shall be liable for any costs incurred by the County because of Contractor's default. The Contractor shall promptly reimburse the County for the full amount of its liability, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract or order with the County.

Notice of Default. In lieu of terminating immediately upon the other Party's default, the non-defaulting Party may, at its option, provide written notice specifying the cause for termination and allow the defaulting Party thirty (30) days (or other specified time period by the County) to cure. If, within thirty (30) days (or other specified time) after the non-defaulting Party has given the Defaulting Party such notice, Defaulting Party has not cured to the satisfaction of the non-Defaulting Party, or if the default cannot be reasonably cured within that time period, non-Defaulting Party may terminate this Agreement at any time thereafter. County shall determine whether Contractor's actions constitute complete or partial cure. In the event of partial cure, County may, at its option, decide whether to (a) give Contractor additional time to cure while retaining the right to immediately terminate at any point thereafter for cause; or (b) terminate immediately for cause. If this Agreement is terminated, neither party may nullify obligations, if any, already incurred prior to the date of termination.

If, after notice of termination under the provisions of this clause, it is determined for any reason that the Contractor was not in default under this provision of this clause, the County has the option to make its notice of termination pursuant to the Termination for Convenience clause and the rights and obligations of the parties would be in accordance with that provision.

Notwithstanding any of the above, if County determines that any action by Contractor contributes to the curtailment of an essential service or pose an immediate threat to life, health, or property, County may terminate this Agreement effective immediately without penalty or opportunity to cure upon issuing either oral or written notice to the Contractor.
Notwithstanding the foregoing, the County may terminate this Agreement immediately pursuant to Paragraph 19 (Immediate Termination for Cause). In the event of Immediate Termination for Cause, the rights and obligations in this Paragraph 18 (Termination for Cause) apply, except for the thirty (30) day notice period and ten (10) day cure period.

19. IMMEDIATE TERMINATION FOR CAUSE

(1) Contractor's failure to comply with all terms and conditions set forth in Section 63 of this Exhibit and Exhibits D, E, F, G, G-1, or H, or failure to require such compliance of its officers, employees, contractors, and agents ("Contractor's personnel") engaged in the 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 access County systems or County Data unless and until its employees sign Exhibits E, F, G-1, and H. If Contractor's employees access County systems or County Data without first signing Exhibits E, F, G-1, and H 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 63 of this Exhibit and Exhibits D, E, F, G, G-1, and H, and shall notify County immediately or no later than 24 hours after learning of any violations. 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.

20. TERMINATION FOR BANKRUPTCY

If Contractor is adjudged to be bankrupt or should have a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of Contractor's insolvency, the County may terminate this Agreement immediately without penalty. For the purpose of this Section, bankruptcy shall mean the filing of a voluntary or involuntary petition of bankruptcy or similar relief from creditors; insolvency; the appointment of a trustee or receiver, or any similar occurrence reasonably indicating an imminent inability to perform substantially all the party's duties under this Agreement. If this Agreement is terminated, neither party may nullify obligations, if any, already incurred prior to the date of termination.

21. BUDGETARY CONTINGENCY

Performance and/or payment by the County pursuant to this Agreement is contingent upon the appropriation by the County of sufficient funds for Deliverables covered by this Agreement. If funding is reduced or deleted by the County for services covered by this Agreement, the County may, at its option and without penalty or liability, terminate this Agreement or offer an amendment to this Agreement indicating the reduced amount.

22. DISENTANGLEMENT

Contractor shall cooperate with County and County's other contractors to ensure a smooth transition at the time of termination of this Agreement, regardless of the nature or timing of the termination. Contractor shall cooperate with County's efforts to ensure that there is no interruption of work required under the Agreement and no adverse impact on the supply of goods, provision of County services or the County activities. Contractor shall return to County all County assets or information in Contractor's possession.

For any software programs developed for use under the County's Agreement, Contractor shall provide a nonexclusive, nontransferable, fully-paid, perpetual, irrevocable, royalty-free worldwide license to the County, at no charge to County, to use, copy, and modify, all work or derivatives that would be needed in order to allow County to continue to perform for itself, or obtain from other providers, the services as the same might exist at the time of termination.

County shall be entitled to purchase at net book value those Contractor assets used for the provision of services to or for County, other than those assets expressly identified by the parties as not being subject to this provision. Contractor shall promptly remove from County's premises, or the site of the work being performed by Contractor for County, any Contractor assets that County, or its designee, chooses not to purchase under this provision.

Contractor shall deliver to County or its designee, at County's request, all documentation and data related to County, including, but not limited to, the County Data and client files, held by Contractor, within sixty (60) days of the request, and after return of same, Contractor shall destroy all copies thereof not turned over to County, all at no charge to County.

23. DISPUTES

Except as otherwise provided in this Agreement, any dispute arising under this contract that is not disposed of by agreement shall be decided by the County's authorized representative or designee, who shall furnish the decision to the Contractor in writing. The decision of the County's authorized representative or designee shall be final and conclusive. The Contractor shall proceed diligently with the performance of the contract pending the County's authorized representative or designee's decision. The County's authorized representative or designee shall not be required to decide issues that are legal or beyond his or her scope of expertise.

24. ACCOUNTABILITY

Contractor will be the primary point of contact for the performance of any subcontractors and assume the responsibility of all matters relating to the purchase of goods and/or services under this Agreement, including payment issues. If such or similar issues arise, the Contractor must take immediate action to correct or resolve the issues.

25. NO ASSIGNMENT, DELEGATION OR SUBCONTRACTING WITHOUT PRIOR WRITTEN CONSENT

Contractor may not assign any of its rights, delegate any of its duties or subcontract any portion of its work or business under this Agreement or any contract release purchase order without the prior written consent of County. No assignment, delegation or subcontracting will release Contractor from any of its obligations or alter any of its obligations to be performed under the Agreement. Any attempted assignment, delegation or subcontracting in violation of this provision is voidable at the option of the County and constitutes material breach by Contractor. As used in this provision, "assignment" and "delegation" means any sale, gift, pledge, hypothecation, encumbrance, or other transfer of all or any portion of the rights, obligations, or liabilities in or arising from this Agreement to any person or entity, whether by operation of law or otherwise, and regardless of the legal form of the transaction in which the attempted transfer occurs.

26. MERGER AND ACQUISITION

The terms of this Agreement will survive an acquisition, merger, divestiture or other transfer of rights involving Contractor. In the event of an acquisition, merger, divestiture or other transfer of rights Contractor must ensure that the acquiring entity or the new entity is legally required to:

(1) Honor all the terms negotiated in this Agreement and any pre-acquisition or pre-merger Agreement between Contractor and the County, including but not limited to a) established pricing and fees; b) guaranteed product support until the contract term even if a new product is released; and c) no price escalation during the term of the contract.

(2) If applicable, provide the functionality of the software in a future, separate or renamed product, if the acquiring entity or the new entity reduces or replaces the functionality, or otherwise provide a substantially similar functionality of the current licensed product. The County will not be required to pay any additional license or maintenance fee to an acquiring entity in order to continue with full use, benefit, and functionality of software licensed under this Agreement until expiration or termination.

(3) Give 30-days written notice to the County following the closing of an acquisition, merger, divestiture or other transfer of right involving Contractor.

27. COMPLIANCE WITH ALL LAWS & REGULATIONS APPLICABLE TO GOODS AND/OR SERVICES PROVIDED

Contractor shall comply with all laws, codes, regulations, rules and orders (collectively, "Regulations") applicable to the goods and/or services to be provided hereunder. Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the contract. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 *et seq.* the Fair Packaging and Labeling Act, and the standards and regulations issued there under. Contractor agrees to indemnify and hold harmless the County for any loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor's

failure to comply with any Regulation applicable to the goods and/or services to be provided hereunder.

28. FORCE MAJEURE

Neither party shall be liable for failure of performance, nor incur any liability to the other party on account of any loss or damage resulting from any delay or failure to perform all or any part of this Agreement if such delay or failure is caused by events, occurrences, or causes beyond the reasonable control and without negligence of the parties. Such events, occurrences, or causes will include acts of God/nature (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, riots, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, lockout, blockage, embargo, labor dispute, strike, interruption or failure of electricity or telecommunication service ("Force Majeure Event").

Each party, as applicable, shall give the other party notice of its inability to perform and reasonable detail of the cause of the inability. Each party must use best efforts to remedy the situation and remove, as soon as practicable, the cause of its inability to perform or comply.

The party asserting a Force Majeure Event as a cause for non-performance shall have the burden of proving that reasonable steps were taken to minimize delay or damages caused by foreseeable events, that all non-excused obligations were substantially fulfilled, and that the other party was timely notified of the likelihood or actual occurrence which would justify such an assertion, so that other prudent precautions could be contemplated.

29. INDEPENDENT CONTRACTOR

Contractor shall supply all goods and/or perform all services pursuant to this Agreement as an independent contractor and not as an officer, agent, or employee of County. Contractor shall be solely responsible for the acts and omissions of its officers, agents, employees, contractors, and subcontractors, if any. Nothing herein shall be considered as creating a partnership or joint venture between the County and Contractor. No person performing any services and/or supplying all goods shall be considered an officer, agent, or employee of County, nor shall any such person be entitled to any benefits available or granted solely to employees of the County.

Contractor is responsible for payment to sub-contractors and must monitor, evaluate, and account for the sub-contractor(s) services and operations.

30. INSURANCE

Contractor shall maintain insurance coverage pursuant to the exhibit setting forth insurance requirements, if such exhibit is attached to the Agreement.

31. DAMAGE AND REPAIR BY CONTRACTOR

Any and all damages to County owned or leased property caused by Contractor's negligence or lack of due care shall be repaired, replaced or reimbursed by Contractor at no charge to the County. Repairs and replacements shall be completed within seventy-two (72) hours of the incident unless the County requests or agrees to an extension or another time frame. The cleanup of all damage related to accidental or intentional release of any/all non-hazardous or hazardous material (e.g. hydraulic fluid, fuel, grease) from Contractor's vehicles or during performance shall be the responsibility of the Contractor. All materials must be cleaned up in a manner and time acceptable to County (completely and immediately to prevent potential as well as actual environmental damage). Contractor must immediately report each incident to the County's Director of Procurement or designee. Damage observed by Contractor, whether or not resulting from Contractor's operations or negligence shall be promptly reported by Contractor to County. County may, at its option, approve and/or dictate the actions that are in County's best interests.

32. LIENS, CLAIMS, ENCUMBRANCES AND TITLE
The Contractor represents and warrants that all the goods and materials ordered and delivered are free and clear of all liens, claims or encumbrances of any kind. Title to the material and supplies purchased shall pass directly from Contractor to County at the F.O.B. point, subject to the right of County to reject upon inspection.

33. ASSIGNMENT OF CLAYTON ACT, CARTWRIGHT ACT CLAIMS
Contractor hereby assigns to the County all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the Contractor for sale to the County pursuant to this Agreement.

34. INDEMNITY
Contractor shall indemnify, defend, and hold harmless the County, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of, or in connection with, performance of this Agreement 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. It is the intent of the parties to this Agreement to provide the broadest possible coverage for the County. Contractor shall reimburse the County for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which Contractor contests its obligation to indemnify, defend and/or hold harmless the County under this Agreement and does not prevail in that contest.

35. INTELLECTUAL PROPERTY INDEMNITY
Contractor represents and warrants for the benefit of the County and its users that it is the exclusive owner of all rights, title and interest in the product or services to be supplied.
Contractor shall, at its own expense, indemnify, defend, settle, and hold harmless the County and its employees, agents and assigns against any claim or potential claim that any good, (including software) and/or service, or County's use of any good (including software) and/or service, provided under this Agreement infringes any patent, trademark, copyright or other proprietary rights, including trade secret rights. Contractor shall pay all costs, damages and attorneys' fees that a court or other adjudicatory body awards as a result of any such claim.

36. WARRANTY
See Exhibit I, section 9.

37. COOPERATION WITH REVIEW
Contractor shall cooperate with County's periodic review of Contractor's performance.

Contractor shall make itself available onsite to review the progress of the project and Agreement, as requested by the County, upon reasonable advanced notice.

Contractor agrees to extend to the County or his/her designees and/or designated auditor of the County, the right to monitor or otherwise evaluate all work performed and all records, including service records and procedures to assure that the project is achieving its purpose, that all applicable County, State, and Federal regulations are met, and that adequate internal fiscal controls are maintained.

38. AUDIT RIGHTS
Pursuant to California Government Code Section 8546.7, the parties acknowledge and agree that every contract involving the expenditure of public funds in excess of $10,000 may be subject to audit by the State Auditor.

All payments made under this Agreement shall be subject to an audit at County's option and shall be

adjusted in accordance with said audit. Adjustments that are found necessary as a result of auditing may be made from current billings.

The Contractor shall be responsible for receiving, replying to, and complying with any payment adjustments set forth in any County audits. The Contractor shall pay to County the full amount determined to be due as a result of a County audit. This provision is in addition to other inspection and access rights specified in this Agreement.

39. ACCESS AND RETENTION OF RECORDS AND PROVISION OF REPORTS

Contractor shall maintain financial records adequate to show that County funds paid were used for purposes consistent with the terms of the contract between Contractor and County. Records shall be maintained during the term of the Agreement and for a period of four (4) years from its termination, or until all claims have been resolved, whichever period is longer, unless a longer period is required under any contract or applicable law.

All books, records, reports, and accounts maintained pursuant to the Agreement, or related to the Contractor's activities under the Agreement, shall be open to inspection, examination, and audit by County, federal and state regulatory agencies, and to parties whose Agreements with the County require such access. County shall have the right to obtain copies of any and all of the books and records maintained pursuant to the Agreement, upon the payment of reasonable charges for the copying of such records.

Contractor shall provide annual reports that include, at a minimum, (i) the total contract release purchase order value for the County as a whole and individual County departments, and (ii) the number of orders placed, the breakdown (by customer ID/department and County) of the quantity and dollar amount of each product and/or service ordered per year. Annual reports must be made available no later than 30 days of the contract anniversary date unless otherwise requested.

Contractor shall also provide quarterly reports to the County that show a breakdown by contract release purchase order (i) the order date (ii) ship date (iii) estimated arrival date (iv) actual arrival date (v) list of products, services and maintenance items and (vi) the number and details of problem/service calls and department name that each such call pertains to (including unresolved problems). Quarterly reports must be made available to the County in electronic format, two (2) business days after the end of each quarter unless otherwise requested.

40. ACCESS TO BOOKS AND RECORDS PURSUANT TO THE SOCIAL SECURITY ACT

Access to Books and Records: If and to the extent that, Section 1861 (v) (1) (1) of the Social Security Act (42 U.S.C. Section 1395x (v) (1) (1) is applicable, Contractor shall maintain such records and provide such information to County, to any payor which contracts with County and to applicable state and federal regulatory agencies, and shall permit such entities and agencies, at all reasonable times upon request, to access books, records and other papers relating to the Agreement hereunder, as may be required by applicable federal, state and local laws, regulations and ordinances. Contractor agrees to retain such books, records and information for a period of at least four (4) years from and after the termination of this Agreement. Furthermore, if Contractor carries out any of its duties hereunder, with a value or cost of Ten Thousand Dollars ($10,000) or more over a twelve (12) month period, through a subcontract with a related organization, such subcontract shall contain these same requirements. This provision shall survive the termination of this Agreement regardless of the reason for the termination.

41. COUNTY NO-SMOKING POLICY

Contractor and its employees, agents and subcontractors, shall comply with the County's No Smoking Policy, as set forth in the Board of Supervisors Policy Manual section 3.47 (as amended from time to time), which prohibits smoking: (1) at the Santa Clara Valley Medical Center Campus and all County-owned and operated health facilities, (2) within thirty (30) feet surrounding County-

owned buildings and leased buildings where the County is the sole occupant, and (3) in all County vehicles.

42. FOOD AND BEVERAGE STANDARDS

Except in the event of an emergency or medical necessity, the following nutritional standards shall apply to any foods and/or beverages purchased by Contractor with County funds for County-sponsored meetings or events.

If food is to be provided, healthier food options shall be offered. "Healthier food options" include (1) fruits, vegetables, whole grains, and low fat and low calorie foods; (2) minimally processed foods without added sugar and with low sodium; (3) foods prepared using healthy cooking techniques; and (4) foods with less than 0.5 grams of trans fat per serving. Whenever possible, Contractor shall (1) offer seasonal and local produce; (2) serve fruit instead of sugary, high calorie desserts; (3) attempt to accommodate special, dietary and cultural needs; and (4) post nutritional information and/or a list of ingredients for items served. If meals are to be provided, a vegetarian option shall be provided, and the Contractor should consider providing a vegan option. If pre-packaged snack foods are provided, the items shall contain: (1) no more than 35% of calories from fat, unless the snack food items consist solely of nuts or seeds; (2) no more than 10% of calories from saturated fat; (3) zero trans-fat; (4) no more than 35% of total weight from sugar and caloric sweeteners, except for fruits and vegetables with no added sweeteners or fats; and (5) no more than 360 mg of sodium per serving.

If beverages are to be provided, beverages that meet the County's nutritional criteria are (1) water with no caloric sweeteners; (2) unsweetened coffee or tea, provided that sugar and sugar substitutes may be provided as condiments; (3) unsweetened, unflavored, reduced fat (either nonfat or 1% low fat) dairy milk; (4) plant-derived milk (e.g., soy milk, rice milk, and almond milk) with no more than 130 calories per 8 ounce serving; (5) 100% fruit or vegetable juice (limited to a maximum of 8 ounces per container); and (6) other low-calorie beverages (including tea and/or diet soda) that do not exceed 40 calories per 8 ounce serving. Sugar-sweetened beverages shall not be provided

43. DEBARMENT

Contractor represents and warrants that it, its employees, contractors, subcontractors or agents (collectively "Contractor") are not suspended, debarred, excluded, or ineligible for participation in Medicare, Medi-Cal or any other federal or state funded health care program, if applicable, or from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration.

Contractor must within thirty (30) calendar days advise the County if, during the term of this Agreement, Contractor becomes suspended, debarred, excluded or ineligible for participation in Medicare, Medi-Cal or any other federal or state funded health care program, as defined by 42. U.S.C. 1320a-7b (f), or from receiving Federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration. Contractor will indemnify, defend and hold the County harmless for any loss or damage resulting from the conviction, debarment, exclusion or ineligibility of the Contractor.

44. CALIFORNIA PUBLIC RECORDS ACT

The County is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Contractor's proprietary information is contained in documents or information submitted to County, and Contractor claims that such information falls within one or more CPRA exemptions, Contractor must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to Contractor prior to such disclosure. If Contractor contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from

a court of law in Santa Clara County before the County is required to respond to the CPRA request. If Contractor fails to obtain such remedy within the time the County is required to respond to the CPRA request, County may disclose the requested information.

Contractor further agrees that it shall defend, indemnify and hold County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorney's fees) that may result from denial by County of a CPRA request for information arising from any representation, or any action (or inaction), by the Contractor.

45. CONFLICT OF INTEREST; POLITICAL REFORM ACT DISCLOSURE REQUIREMENT

If applicable, Contractor shall comply with all applicable requirements governing avoidance of impermissible client conflicts; and federal, state and local conflict of interest laws and regulations including, without limitation, California Government Code section 1090 *et seq.*, the California Political Reform Act (California Government Code section 87100 *et seq.*) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 *et seq.*). Failure to do so constitutes a material breach of this Agreement and is grounds for immediate termination of this Agreement by the County.

In accepting this Agreement, Contractor covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this Agreement. Contractor further covenants that, in the performance of this Agreement, it will not use any contractor or employ any person having such an interest. Contractor, including but not limited to contractor's employees, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under this Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

Contractor, including but not limited to contractor's employees and subcontractors, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under the Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

If the disclosure provisions of the Act are applicable to any individual providing service under the Agreement, Contractor shall, upon execution of the Agreement, provide the County with the names, description of individual duties to be performed, and email addresses of all individuals, including but not limited to Contractor's employees, agents and subcontractors, that could be substantively involved in "making a governmental decision" or "serving in a staff capacity and in that capacity participating in making governmental decisions or performing duties that would be performed by an individual in a designated position," as part of Contractor's service to the County under the Agreement. Contractor shall ensure that such individuals file Statements of Economic Interests within 30 days of commencing service under the Contract, annually by April 1, and within 30 days of their termination of service under the Contract.

46. SEVERABILITY

Should any part of this Agreement between County and the Contractor or any individual contract release purchase order be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect the validity of the remainder of the Agreement or any individual contract release purchase order which shall continue in full force and effect, provided that such remainder can, absent the excised portion, be reasonably interpreted to give the effect to the intentions of the parties.

47. NON-WAIVER
No waiver of a breach, failure of any condition, or any right or remedy contained in or granted by the provisions of this Agreement will be effective unless it is in writing and signed by County. No waiver of any breach, failure, right, or remedy will be deemed a waiver of any other breach, failure, right, or remedy, whether similar or not, nor will any waiver constitute a continuing waiver unless the writing signed by the County so specifies.

48. USE OF COUNTY'S NAME FOR COMMERCIAL PURPOSES
Contractor may not use the name of the County or reference any endorsement from the County in any fashion for any purpose, without the prior express written consent of the County as provided by the County's authorized representative, or designee.

49. HEADINGS AND TITLES
The titles and headings in this Agreement are included principally for convenience and do not by themselves affect the construction or interpretation of any provision in this Agreement, nor affect any of the rights or obligations of the parties to this Agreement.

50. HANDWRITTEN OR TYPED WORDS
Handwritten or typed words have no greater weight than printed words in the interpretation or construction of this Agreement.

51. AMBIGUITIES
Any rule of construction to the effect that ambiguities are to be resolved against the drafting party does not apply in interpreting this Agreement.

52. ENTIRE AGREEMENT; MERGER
This Agreement and its Exhibits and Attachments (if any) constitute the final, complete and exclusive statement of the terms of the agreement between the parties. It incorporates and supersedes all the agreements, covenants and understandings between the parties concerning the subject matter hereof, and all such agreements, covenants and understandings have been merged into this Agreement. No prior or contemporaneous agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

53. EXECUTION AND COUNTERPARTS
This Agreement may be executed in one or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. The parties agree that this Agreement, its amendments, and ancillary agreements to be entered into in connection with this Agreement will be considered signed when the signature of a party is delivered a method described herein.

Unless otherwise prohibited by law or County policy, the parties agree that an electronic copy of a signed contract, or an electronically signed contract, has the same force and legal effect as a contract executed with an original ink signature. The term "electronic copy of a signed contract" refers to a transmission by facsimile, electronic mail, or other electronic means of a copy of an original signed contract in a portable document format. The term "electronically signed contract" means a contract that is executed by applying an electronic signature using technology approved by the County.

54. NOTICES
All deliveries, notices, requests, demands or other communications provided for or required by this Agreement shall be in writing and shall be deemed to have been given when sent by registered or certified mail, return receipt requested; when sent by overnight carrier; or upon email confirmation to sender of receipt of a facsimile communication which is followed by a mailed hard copy from sender. Notices shall be addressed to the individuals identified in the Key Provisions of the Agreement as the County Contract Administrator and the Supplier Contact. Each party may designate a different

person and address by sending written notice to the other party, to be effective no sooner than ten (10) days after the date of the notice.

55. ACCOUNT MANAGER
Contractor must assign an Account Manager to the County upon execution of the Agreement to facilitate the contractual relationship, be fully responsible and accountable for fulfilling the County's requirements. Contractor represents and warrants that such person will ensure that the County receives adequate pre-sales and post-sales support, problem resolution assistance and required information on a timely basis.

56. SURVIVAL
All representations, warranties, and covenants contained in this Agreement, or in any instrument, certificate, exhibit, or other writing intended by the parties to survive this Agreement, will survive the termination of this Agreement.

57. GOVERNING LAW, JURISDICTION AND VENUE
This Agreement shall be construed and interpreted according to the laws of the State of California, excluding its conflict of law principles. Proper venue for legal actions shall be exclusively vested in state court in the County of Santa Clara. The parties agree that subject matter and personal jurisdiction are proper in state court in the County of Santa Clara, and waive all venue objections.

58. THIRD PARTY BENEFICIARIES
This Agreement does not, and is not intended to, confer any rights or remedies upon any person or entity other than the parties

59. AUTHORITY
Each party executing the Agreement on behalf of such entity represents that he or she is duly authorized to execute and deliver this Agreement on the entity's behalf, including, as applicable, the Board of Supervisors, the Board of Directors, or Executive Director. This Agreement shall not be effective or binding unless it is in writing and approved by the County's authorized representative, or authorized designee, as evidenced by their signature as set forth in this Agreement.

60. LIVING WAGE
Unless otherwise exempted or prohibited by law or County policy, Contractors that contract with the County to provide Direct Services, as defined in County of Santa Clara Ordinance Code Division B36 ("Division B36") and Board Policy section 5.5.5.5 ("Living Wage Policy"), and their subcontractors, where the contract value is $100,000 or more, must comply with Division B36 and the Living Wage Policy and compensate their employees in accordance with Division B36 and the Living Wage Policy. Compliance and compensation for purposes of this provision includes, but is not limited to, components relating to fair compensation, earned sick leave, paid jury duty, fair workweek, worker retention, fair chance hiring, targeted hiring, local hiring, protection from retaliation, and labor peace. If Contractor and/or a subcontractor violate this provision, the Board of Supervisors or its designee may, at its sole discretion, take responsive actions including, but not limited to, the following:
(1) Suspend, modify, or terminate the Direct Services Contract.
(2) Require the Contractor and/or Subcontractor to comply with an appropriate remediation plan developed by the County.
(3) Waive all or part of Division B36 or the Living Wage Policy.

This provision shall not be construed to limit an employee's rights to bring any legal action for violation of the employee's rights under Division B36 or any other applicable law. Further, this provision does not confer any rights upon any person or entity other than the Board of Supervisors or its designee to bring any action seeking the cancellation or suspension of a County contract. By entering into this contract, Contractor certifies that it is currently complying with County Code

Division B36 and the County's Living Wage Policy with respect to applicable contracts, and warrants that it will continue to comply with County Code Division B36 and the County's Living Wage Policy with respect to applicable contracts.

61. CONTRACTING PRINCIPLES
All entities that contract with the County to provide services where the contract value is $100,000 or more per budget unit per fiscal year and/or as otherwise directed by the Board, shall be fiscally responsible entities and shall treat their employees fairly. To ensure compliance with these contracting principles, all contractors shall: (1) comply with all applicable federal, state and local rules, regulations and laws: (2) maintain financial records, and make those records available upon request; (3) provide to the County copies of any financial audits that have been completed during the term of the Agreement; (4) upon the County's request, provide the County reasonable access, through representatives of the Contractor, to facilities, financial and employee records that are related to the purpose of the Agreement, except where prohibited by federal or state laws, regulations or rules.

62. CONTRACTOR TRAVEL EXPENSES
Contractor shall be solely responsible for any travel fees or out of pocket.

63. INFORMATION SECURITY COMPLIANCE
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.

64. COUNTY DATA
(1) Contractor shall not acquire any ownership interest in County Data (including County Confidential Information). As between Contractor and County, all County Confidential Information and/or County 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) other than in the performance of its obligations under this Agreement.

(2) Contractor shall be responsible for establishing and maintaining an information security program that is designed to ensure the security and confidentiality of County Data, protect against any anticipated threats or hazards to the security or integrity of County 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. Upon termination or expiration of this Agreement, Contractor shall seek and follow County's direction regarding the proper

disposition of County Data.

(3) Contractor shall take appropriate action to address any incident of unauthorized access to County 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 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 and/or legally protected County 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.

(4) 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.

65. ACCESS TO COMPETITIVELY BID AGREEMENTS

Where the contract award is a result of a formal competitive solicitation, Contractor may opt to permit the use of this Agreement by other political subdivisions, municipalities, tax supported agencies and non-profit entities in the United States. Such participating agencies shall make purchases in their own name, make payments directly to the Contractor and shall be liable directly to Contractor holding the County of Santa Clara harmless.

If applicable, Contractor shall be required to maintain a list of cooperative entities using this Agreement. The list shall report dollar volumes spent annually and shall be provided on an annual basis to the County, at the County's request.

66. COMPLIANCE WITH ALL LAWS AND REGULATIONS INCLUDING NONDISCRIMINATION, EQUAL OPPORTUNITY, AND WAGE THEFT PREVENTION

Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the Agreement. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 *et seq.* the Fair Packaging and Labeling Act. and the standards and regulations issued there under. Contractor agrees to indemnify and hold harmless the County for any loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor's failure to comply with the act and any standards or regulations issued there under.

(1) Compliance with All Laws. Contractor shall comply with all applicable Federal, State, and local laws, regulations, rules, and policies (collectively, "Laws"), including but not limited to the non-discrimination, equal opportunity, and wage and hour Laws referenced in the paragraphs below.

(2) Compliance with Non-Discrimination and Equal Opportunity Laws: Contractor shall comply with all applicable Laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Santa Clara County's policies for contractors on nondiscrimination and equal opportunity; Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and 504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Government Code sections 12900 et seq.); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information

Nondiscrimination Act of 2008. In addition to the foregoing, Contractor shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall Contractor discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

(3) Compliance with Wage and Hour Laws: Contractor shall comply with all applicable wage and hour Laws, which may include but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and, if applicable, any local Minimum Wage, Prevailing Wage, or Living Wage laws.

(4) Definitions: For purposes of this Section, the following definitions shall apply. A "Final Judgment, Decision, Determination, or Order" shall mean a judgment, decision, determination, or order (a) which is issued by a court of law, an investigatory government agency authorized by law to enforce an applicable Law, an arbiter, or arbitration panel and (b) for which all appeals have been exhausted or the time period to appeal has expired. For pay equity Laws, relevant investigatory government agencies include the federal Equal Employment Opportunity Commission, the California Division of Labor Standards Enforcement, and the California Department of Fair Employment and Housing. Violation of a pay equity Law shall mean unlawful discrimination in compensation on the basis of an individual's sex, gender, gender identity, gender expression, sexual orientation, race, color, ethnicity, or national origin under Title VII of the Civil Rights Act of 1964 as amended, the Equal Pay Act of 1963, California Fair Employment and Housing Act, or California Labor Code section 1197.5, as applicable. For wage and hour Laws, relevant investigatory government agencies include the federal Department of Labor, the California Division of Labor Standards Enforcement, and the City of San Jose's Office of Equality Assurance.

(5) Prior Judgments, Decisions or Orders against Contractor: By signing this Agreement, Contractor affirms that it has disclosed any final judgments, decisions, determinations, or orders that (a) were issued in the five years prior to executing this Agreement by a court or investigatory government agency and (b) found that Contractor violated an applicable wage and hour or pay equity law. Contractor further affirms that it has satisfied and complied with – or has reached agreement with the County regarding the manner in which it will satisfy – any such final judgments, decisions, determinations, or orders.

(6) Violations of Wage and Hour Laws or Pay Equity Laws During Term of Agreement: If at any time during the term of this Agreement, Contractor receives a Final Judgment, Decision, Determination, or Order rendered against it for violation of an applicable wage and hour Law or pay equity Law, then Contractor shall promptly satisfy and comply with any such Final Judgment, Decision, Determination or Order. Contractor shall inform the Office of the County Executive-Office of Countywide Contracting Management (OCCM) of any relevant Final Judgment, Decision, Determination, or Order against it within 30 days of the Final Judgment, Decision, Determination, or Order becoming final or of learning of the Final Judgment, Decision, Determination, or Order, whichever is later. Contractor shall also provide any documentary evidence of compliance with the Final Judgment, Decision, Determination, or Order within 5 days of satisfying the Final Judgment, Decision, Determination, or Order. Any notice required by this paragraph shall be addressed to the Office of the County Executive-OCCM at 70 W. Hedding Street, East Wing, 11th Floor, San José, CA 95110. Notice provisions in this paragraph are separate from any other notice provisions in this Agreement and, accordingly, only notice

provided to the Office of the County Executive-OCCM satisfies the notice requirements in this paragraph.

(7) Access to Records Concerning Compliance with Pay Equity Laws: In addition to and notwithstanding any other provision of this Agreement concerning access to Contractor's records, Contractor shall permit the County and/or its authorized representatives to audit and review records related to compliance with applicable pay equity Laws. Upon the County's request, Contractor shall provide the County with access to any and all facilities and records, including but not limited to financial and employee records, that are related to the purpose of this Section, except where prohibited by federal or state laws, regulations or rules. County's access to such records and facilities shall be permitted at any time during Contractor's normal business hours upon no less than 10 business days' advance notice.

(8) Pay Equity Notification: Contractor shall (1) directly provide each employee working in California and each person applying for a job in California with a written copy of any applicable pay equity Laws, or (2) electronically disseminate the text of applicable pay equity Laws to each California employee and job applicant, either directly or by posting a copy in conspicuous places available to employees and applicants. Such notification shall occur at least once during the term of this Agreement and, if this Agreement is a multi-year Agreement, at least annually thereafter.

(9) Material Breach: Failure to comply with any part of this Section shall constitute a material breach of this Agreement. In the event of such a breach, the County may, in its discretion, exercise any or all remedies available under this Agreement and/or at law. County may, among other things, take any or all of the following actions:
   (i) Suspend or terminate any or all parts of this Agreement.
   (ii) Withhold payment to Contractor until full satisfaction of a Final Judgment, Decision, Determination, or Order.
   (iii) Offer Contractor an opportunity to cure the breach.

(10) Subcontractors: Contractor shall impose all of the requirements set forth in this Section on any subcontractors permitted to perform work under this Agreement. This includes ensuring that any subcontractor receiving a Final Judgment, Decision, Determination, or Order for violation of an applicable wage and hour Law promptly satisfies and complies with such Final Judgment, Decision, Determination, or Order.

EXHIBIT B
MAINTENANCE FEES SCHEDULE

Idemia agrees to interface the AFIS and Live Scan with the replacement system to CJIC mainframe, the latter of which is being decommissioned in the next couple of years, at no additional cost to the County.

Maintenance Schedule for July 1, 2019 through June 30, 2020

Location	Node	Product	Maintenance Fee
Contract #24836			**July 1, 2019 - June 30, 2020**
Campbell PD - Remote	SALP23	Lexmark Tenprint Card Printer	$347.29
Elmwood-Processing	SALP10	Lexmark Tenprint Card Printer	$347.29
Los Altos PD - Remote	SALP14	Lexmark Tenprint Card Printer	$347.29
Los Gatos PD - Remote	SALP22	Lexmark Tenprint Card Printer	$347.29
Milpitas PD - Remote	SALP34	Lexmark Tenprint Card Printer	$347.29
Morgan Hill PD - Remote	SALP19	Lexmark Tenprint Card Printer	$347.29
Palo Alto PD - Remote	SALP13	Lexmark Tenprint Card Printer	$347.29
San Jose PD- Juvenile Processing	SALP27	Lexmark Tenprint Card Printer	$347.29
Santa Clara SO	SALP00	Lexmark Tenprint Card Printer	$347.29
San Jose PD- Adult Processing	SALP01	Lexmark Tenprint Card Printer	$347.29
Santa Clara SO	SALP02	Lexmark Tenprint Card Printer	$347.29
San Jose PD-RM 206	SALP03	Lexmark Tenprint Card Printer	$347.29
San Jose PD-Rm 204	SALP25	Lexmark Tenprint Card Printer (Lexmark T630)	$347.29
Santa Clara Probation Dep - Adult	SALP35	Lexmark Tenprint Card Printer	$347.29
Santa Clara County - South	SALP21	Lexmark Tenprint Card Printer	$347.29
Santa Clara Probation Dep – Juv	SALP36	Lexmark Tenprint Card Printer	$347.29
Campbell PD - Remote	SALV23	LSS4000R	$3,956.11
Elmwood-Processing	SALV10	LSS4000N	$4,798.38
Los Altos PD - Remote	SALV14	LSS4000R	$3,956.11
Los Gatos PD - Remote	SALV22	LSS4000R	$3,956.11

Milpitas PD - Remote	SALV34	LSS4000N	$3,956.11
Morgan Hill PD - Remote	SALV19	LSS4000R	$4,798.38
Palo Alto PD - Remote	SALV13	LSS4000R	$3,956.11
San Jose PD - Juvenile Processing	SALV27	LSS4000N	$4,798.38
San Jose PD- Adult Processing	SALV12	LSS4000N	$4,798.38
San Jose PD-Rm 204	SALV25	LSS4000R	$4,798.38
Santa Clara SO	SALV24	LSS4000R	$3,828.50
Santa Clara Probation Dep - Adult	SALV35	LSS4000R	$3,956.11
Santa Clara Probation Dep – Juv	SALV36	LSS4000R	$4,798.38
South County SO - Remote	SALV21	LSS4000R	$3,956.11
Santa Clara DOC-Main Jail Men's Intake	SAID01	IDS	$1,824.64
Elmwood Men's Intake & Release	SAID02	IDS	$1,824.64
Elmwood Women's Release	SAID03	IDS	$1,824.64
Santa Clara DOC-Release	SAID04	IDS	$1,824.64
Maintenance Subtotal			**$73,166.75**

Location	Node	Product	Maintenance Fee
Contract #19395			**July 1, 2019 - June 30, 2020**
San Jose PD-Rm 204	SALV03	LSS4000R	$4,358.36
Santa Clara SO	SALV05	LSS4000R	$4,358.36
Santa Clara DOC-Main Jail Commit Desk	SALV07	LSS4000R	$4,358.36
Santa Clara DOC-Main Jail Intake	SALV11	LSS4000R	$4,358.36
Mt View PD - Remote	SALV15	LSS4000R	$4,358.36
Santa Clara PD	SALV16	LSS4000R	$4,358.36
Gilroy PD - Remote	SALV20	LSS4000N	$4,358.36
Sunnyvale DPS - Remote	SALV26	LSS4000N	$4,358.36

Santa Clara DOC-Women Intake	SALV32	LSS4000N	$4,358.36
Santa Clara DOC-Men Jail Intake	SALV33	LSS4000N	$3,913.10
Santa Clara SO	SALP05	Lexmark Tenprint Card Printer	$354.23
Santa Clara DOC-Men Jail Intake	SALP11	Lexmark Tenprint Card Printer	$354.23
Mt View PD - Remote	SALP15	Lexmark Tenprint Card Printer	$421.48
Santa Clara PD - Remote	SALP16	Lexmark Tenprint Card Printer	$354.23
Gilroy PD - Remote	SALP20	Lexmark Tenprint Card Printer	$354.23
Sunnyvale DPS - Remote	SALP26	Lexmark Tenprint Card Printer	$354.23
Maintenance Subtotal			**$45,330.99**

Location	Node	Product	Maintenance Fee
Contract #25288			**July 1, 2019 - June 30, 2020**
Santa Clara SO	SCCOADS101	ADS	$79,651.22
Santa Clara SO		Tape Library	$855.45
Santa Clara SO	SCCOBDC101	Backend-Cluster Server	$182.31
Santa Clara SO		SAN - Storage Area Network	$4,347.38
Santa Clara SO	SCCODC101	Backend-MBSS-Primary	$322.55
Santa Clara SO	SCCOBUS101	Backup Server	$182.31
Santa Clara SO	SCCODES101	DES + DPS	$11,532.86
Santa Clara SO	SCCOWS001	Latent Station	$12,507.51
Santa Clara SO	SCCOWS002	Latent Station	$12,507.51
Santa Clara SO	SCCOWS003	Latent Station	$12,507.51
Santa Clara SO	SCCOMBSS101	Matcher Server	$26,205.39
Santa Clara SO	SCCOMBSS102	Matcher Server	$26,205.39
Santa Clara SO	SCCOMBSS103	Matcher Server	$26,205.39
Santa Clara SO	SCCOMBSS104	Matcher Server	$26,205.39
Santa Clara SO	SCCOMBSS105	Matcher Server	- $26,205.39

Santa Clara SO	SCCOPDC101	Primary Domain Controller	$203.35
Santa Clara SO	SCCOWAS101	Web Application Server	$259.44
Santa Clara SO	SALPC01	Color Laser Printer	$173.25
Maintenance Subtotal			**$266,259.57**

Contract #36119		**July 1, 2019 - June 30, 2020**
	Review Station licenses*	$1,575.00
	Review Station licenses	$1,575.00
Maintenance Subtotal		**$3,150.00**
	SUBTOTAL:	**$ 387,907.32**
	ONE-TIME DISCOUNT:	**$ (25,000.00)**
	FULL TERM GRAND TOTAL:	**$ 362,907.32**

*Review Station licenses provide access to the MorphoBIS Server subsystem, allowing operators to review fingerprints, palmprints, and the contents of person and incident records. Operators access the MorphoBIS Home Page through the Reviewer application, and perform search verification, quality control, database maintenance, and record comparison.

**PO EP103297 in the amount of $90,723.83 was issued on July 1, 2019 to cover Maintenance Fees for period July 1, 2019 to September 30, 2019.

The total cost of the five-year maintenance is as follows:

Term Date	AFIS, Live Scan and Printer Maintenance	Active/Passive DR System Maintenance	Annual One Time Discount	Maintenance Total
October 1, 2019 through June 30, 2020	$ 297,183.49	$ 0	$ 25,000.00	$ 272,183.49
July 1, 2020 through June 30, 2021	$ 407,302.69	$ 200,000.00	$ 25,000.00	$ 582,302.69
July 1, 2021 through June 30, 2022	$ 427,667.82	$ 106,720.00	$ 25,000.00	$ 509,387.82
July 1, 2022 through June 30, 2023	$ 449,051.21	$ 110,494.00	$ 25,000.00	$ 534,545.21
July 1, 2023 through June 30, 2024	$ 471,503.77	$ 114,456.00	$ 25,000.00	$ 560,959.77
			Grand Total	**$2,459,378.98**

Maintenance Services

STANDARD SUPPORT

***Advantage* – Software Support**

- Telephone Response: 2 Hour
- Remote Dial-In Analysis
- Unlimited Telephone Support
- Standard Releases & Updates
- Software Customer Alert Bulletins
- Automatic Call Escalation
- Supplemental Releases & Updates
- 8 a.m. – 5 p.m. Monday to FridayPPM**

On-Site Hardware Support

- 8 a.m. – 5 p.m. Monday to FridayPPM
- Next Day PPM On-site Response
- Hardware Vendor Liaison
- Defective Parts Replacement
- Escalation Support
- Hardware Customer Alert Bulletins
- Hardware Service Reporting
- Product Repair
- Equipment Inventory Detail Management

Parts Support

Maintenance and Support Agreement # 001443-000 Rev3 **Date** May

New Term Effective **Start** October 1, 2019 **End** June 30, 2024

** If customer is providing their own on-site hardware support, the following applies:*

- Customer Orders & Replaces Parts ➢ Telephone Technical Support for Parts ReplacementAvailable

**Principal Period of Maintenance (PPM) means the specified days, and times during the days that maintenance and support services will be provided under this Agreement.

ADDITIONAL OPTIONS

Uplifts

- Increase PPM to 24X7 for both Hardware and Software for both Central and Remote
- Increase Response Time to 1 Hour Telephone Response and 4 Hour on-site Response

EXHIBIT C

INSURANCE REQUIREMENTS

Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. Evidence of Coverage

Prior to commencement of this Agreement, the Contractor shall provide a Certificate of Insurance certifying that coverage as required herein has been obtained. Individual endorsements executed by the insurance carrier shall accompany the certificate.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. Qualifying Insurers

All coverages, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation

All coverage as required herein shall not be canceled or changed so as to no longer meet the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

   a. Each occurrence - $1,000,000

   b. General aggregate - $2,000,000

c. Products/Completed Operations aggregate - $1,000,000

d. Personal Injury - $1,000,000

2. General liability coverage shall include:

a. Premises and Operations

b. Personal Injury liability

c. Products/Completed

d. Severability of interest

3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

Additional Insured Endorsement, which shall read:

"County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds."

Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance

For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to owned, non-owned and hired vehicles.

4a. Aircraft/Watercraft Liability Insurance (Required if Contractor or any of its agents or subcontractors will operate aircraft or watercraft in the scope of the Agreement)

For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to all owned non-owned and hired aircraft/watercraft.

5. Workers' Compensation and Employer's Liability Insurance

a. Statutory California Workers' Compensation coverage including broad form all-states coverage.

b. Employer's Liability coverage for not less than one million dollars ($1,000,000) per occurrence.

6. Professional Errors and Omissions Liability Insurance

   a. Coverage shall be in an amount of not less than one million dollars ($1,000,000) per occurrence/aggregate.

   b. If coverage contains a deductible or self-retention, it shall not be greater than fifty thousand dollars ($50,000) per occurrence/event.

   c. Coverage as required herein shall be maintained for a minimum of two years following termination or completion of this Agreement.

7. Cyber Liability

   a. Each occurrence - $1,000,000

   b. General aggregate - $2,000,000

8. Cyber liability coverage shall include at a minimum, but not limited to:

   a. Information Security and Privacy Liability

   b. Privacy Notification Costs

9. Claims Made Coverage

If coverage is written on a claims made basis, the Certificate of Insurance shall clearly state so. In addition to coverage requirements above, such policy shall provide that:

   a. Policy retroactive date coincides with or precedes the Contractor's start of work (including subsequent policies purchased as renewals or replacements).

   b. Policy allows for reporting of circumstances or incidents that might give rise to future claims.

E. Special Provisions

The following provisions shall apply to this Agreement:

1. The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning

indemnification.

2. The County acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractor's obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.

3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned coverages, or Contractor may insure subcontractors under its own policies.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

EXHIBIT D

County Security Addendum

1. Definitions

A. "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.

B. "Contractor Processing Resources" means any user or component of a System that processes County Data.

C. "Contractor Managed Systems" means any System that is managed by Contractor.

D. "Contractor Personnel" means Contractor's officers, employees, agents, and contractors.

E. "Security Incident" shall mean an event that results in, or which Contractor reasonably believes may result in, unauthorized access to, use, modification and/or disclosure of County Data.

F. "Strong password" means a password that meets or exceeds the following criteria:

(i) minimum password length is twelve (12) characters;
the password must be high complexity (contains one of each, upper, lower, number, symbol);
(ii) password must be rotated every ninety (90) days;
(iii) user must not reuse the last ten (10) passwords;
(iv) not be a dictionary word or proper name;
(v) not be transmitted in the clear outside the secure location;
(vi) not be displayed when entered; and
(vii) access to County System is denied after five (5) failed logon attempts.

G. "Systems" include but are not limited to, 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 data.

2. Information Security Management Program and Policies

A. Contractor Security Contact. Contractor shall provide a security representative as a point of contact for County on any security issues.

B. Policies and Procedures. Contractor shall maintain and follow written security management policies and procedures to prevent, detect, contain, and correct violations of

measures taken to protect the confidentiality, integrity, and availability of Contractor Processing Resources and/or County Data. These policies and procedures shall:

(i) assign specific data security responsibilities and accountabilities to specific individual(s);

(ii) include a risk management program that includes periodic risk assessments;

(iii) include a process to respond to the threats and vulnerabilities identified in the risk assessment to mitigate or remediate identified risks to an acceptable level; and

(iv) implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in compliance with all applicable federal, state, and local regulations.

C. Infrastructure Protection. Contractor shall maintain policies and procedures to protect its Processing Resources, including:

(i) security programs (policies, standards, processes, procedures, etc.);

(ii) processes for becoming aware of, and maintaining, security patches and fixes;

(iii) procedures for employing router filters, firewalls, and other mechanisms to restrict access to Contractor Processing Resources, including all local-site networks that may be accessed via the Internet (whether or not such sites transmit information);

(iv) procedures for ensuring that resources used for mobile access have technology installed that is designed to protect against attack, penetration, and compromise (e.g. firewalls, encryption);

(v) processes designed to prevent, detect, and eradicate malicious software; and

(vi) procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

3. Access Control

A. Identification and Authentication. Access to County Data or any Contractor Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes that establish the identity of the person requesting access to County Data and/or Contractor Processing Resources. "Authentication" refers to processes that validate the purported identity of the requestor. For access to County Data or Contractor Processing Resources, except for the LiveScan terminals, Contractor shall require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique. Contractor shall maintain procedures for the protection, integrity, and complexity of any passwords created by Contractor and/or used by Contractor in connection with the performance of Services. Passwords shall, at minimum, meet the complexity requirements of a Strong Password.

B. Account Administration. Contractor shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Contractor Processing Resources and County Data, and shall include procedures for granting and revoking emergency access to Contractor Processing Resources.

C. Access Control. Contractor shall maintain appropriate access control mechanisms to prevent access to County Data and/or Contractor Processing Resources, except by authorized users. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Contractor shall maintain processes to revoke access to County data within 24 hours after any Contractor Personnel are terminated, or immediately in the case of a non-voluntary termination. Contractor shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized access to, or attempts to access, County Data or Contractor Processing Resources.

4. Personnel Security

A. Access to County Data. Contractor shall require Contractor Personnel who have, or may be expected to have, access to County Data or Contractor Processing Resources to comply with the provisions of the Agreement, including this Addendum. Contractor shall remain responsible for any breach of this Addendum by its Personnel.

B. Security Awareness. Contractor shall ensure that Contractor Personnel remain aware of its security practices, and their responsibilities for protecting County Data and Contractor Processing Resources. This shall include Contractor providing security and privacy training as appropriate and Contractor ensuring that its Contractor Personnel are aware of the following:

(i) practices to protect against any form of malicious software;

(ii) appropriate password protection and password management practices; and

(iii) appropriate use of workstations and computer system accounts.

C. Sanction Policy. Contractor shall maintain a sanction policy to address violations by Contractor Personnel of Contractor's internal security requirements or security requirements that are imposed on Contractor by law or contract, including this Agreement.

5. Risk Management

A. General Requirements. Contractor shall maintain appropriate safeguards and controls and exercise due diligence to protect County Data and Contractor Processing Resources against unauthorized access, use, and/or disclosure, considering:

(i) applicable law;

(ii) information technology industry practices;

(iii) the sensitivity of the data; and

(iv) the relative level and severity of risk of impact should the integrity, confidentiality, or availability of the data be compromised, as determined by Contractor as part of an overall risk management program.

B. Security Evaluations. Contractor shall periodically evaluate its processes and systems to ensure continued compliance with obligations imposed by law or contract (including this Agreement) with respect to the confidentiality, integrity, and availability of County Data and Contractor Processing Resources. Contractor shall document the results of these evaluations and any remediation activities taken in response to these evaluations.

C. Internal Records. Contractor shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Contractor shall take appropriate action to address and remediate identified vulnerabilities to County Data and Contractor Processing Resources.

D. Audits. In addition to any audit rights in the Agreement, Contractor shall permit audits at the request of the County to evaluate compliance with this Addendum.

6. Physical Security

A. Contractor shall maintain appropriate physical security controls (including facility and environmental controls) designed to prevent unauthorized physical access, tampering and theft to Contractor Processing Resources and areas in which County Data is stored or processed. Contractor shall adopt and implement a written facility security plan that documents these controls and the policies and procedures through which these controls will be maintained. Contractor shall maintain appropriate records of maintenance performed on Contractor Processing Resources and on the physical control mechanisms used to secure Contractor Processing Resources.

7. Communications Security

A. Exchange of Confidential Information. The parties shall utilize a secure method of transmission when exchanging County Data electronically.

B. Encryption. Contractor shall adhere to the following encryption standards for all County Data:

(i) All County data that is processed and/or stored shall be protected using a Federal Information Processing Standard (FIPS) certified algorithm using a cipher key strength of at least 256 bit; and

(ii) All County data that is transmitted shall be protected using a FIPS certified algorithm using a cipher key strength of at least 128 bit.

C. Protection of Storage Media. Contractor shall ensure that storage media containing County Data is properly and adequately sanitized (through the use of industry standard destruction software) of all County Data or is destroyed prior to disposal or re-use for non-Contractor processing and shall provide the County with the Certificate of Destruction or Sanitization described in section 6(E)(iii) below. All media on which County Data is stored shall be protected against unauthorized access or modification. Contractor shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Contractor processing or on which County Data has been stored.

D. Data Integrity. Contractor shall maintain processes designed to prevent unauthorized or inappropriate modification or destruction of County Data. Contractor shall, at its expense, use commercially reasonable efforts to correct any Data that has been corrupted by unauthorized or inappropriate modification of destruction.

E. Data Return or Destruction.

(i) Upon termination of the Agreement for any reason, Contractor shall, at the option of Covered Entity, immediately return or destroy all County Data that

Contractor or its agents or subcontractors still maintain in any form, and shall retain no copies of such County Data.

(ii) If County elects destruction of such County Data, Contractor shall use any method of confidential destruction meeting the National Institute of Standards and Technology's (NIST) Guidelines for Media Sanitation in Special Publication 800-88, Revision 1, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media for electronic file destruction.

(iii) Contractor will provide the County with a Certificate of Destruction or Sanitization of County Data that identifies the method of destruction or sanitization within 14 days of when the destruction of County Data occurs. Contractor shall include the following information in the Certificate of Destruction:

(a) ***Listing of personnel who reviewed and approved sanitization and disposal actions;***

(b) ***Types of media sanitized or destroyed;***

(c) ***Specific files stored on the media;***

(d) ***Sanitization/Destruction methods used;***

(e) ***Date and time of the Sanitization actions;***

(f) ***Personnel who performed the sanitization;***

(g) ***Verification actions taken;***

(h) ***Personnel who performed the verification; and***

(i) ***Disposal action taken.***

8. Security Incident Monitoring and Response

A. Security Incident Response. Contractor shall maintain processes to detect, identify, report, respond to, and resolve Security Incidents in a timeframe consistent with guidance provided by US-CERT (https://www.us-cert.gov/government-users/reporting-requirements).

B. Security Incident Notification and Privacy Incident Notification. Contractor shall notify the County, as specified below, of any Security Incident(s) that result in, or which Contractor reasonably believes may result in, unauthorized access to, modification of, or disclosure of County Data. Contractor shall report to County in writing any access, use or disclosure of County Data not permitted by the Agreement and this Addendum of which it becomes aware without unreasonable delay and in no case later than 24 hours after discovery. All reports to County pursuant to this section shall be via email to the County Information Security Office, o365-iso-team@sccconnect.onmicrosoft.com.

Contractor must send to County within 5 days of discovery a full notice that must contain: (i) a brief description of what happened, including the date of the Incident and the date of the discovery (ii) the location of the Incident; (iii) a description of the types of County Data that were involved in the Incident, (iv) safeguards in place prior to the Incident; (v) Actions taken in response

to the Incident; (vi) a brief description of what the Contractor is doing to investigate the Incident, to mitigate harm to individuals, and to protect against further Incidents, and (vii) any other information established by the standards for US-CERT incident response.

9. Indemnification

A. In addition to the indemnification language in the Agreement, Contractor agrees (i) to be responsible for, and defend, indemnify and hold harmless the County, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of, or in connection with, any breach of Contractor's privacy or security obligations under the Agreement, including any fines, penalties, and assessments that may be made against County or Contractor for any Privacy or Security Incidents or late reporting; and (ii) to pay and bear responsibility for the cost of and notice for any credit monitoring services.

10. Contractor Managed System Requirements

A. Vulnerability and Patch Management

(i) For all Contractor Managed Systems, Contractor shall install and maintain certified anti-virus software and, to the extent possible, use real time protection features. Contractor shall maintain the Anti-virus software in accordance with the anti-virus software vendor's recommended practices. In addition, Contractor shall ensure that: (a) the anti-virus software checks for new anti-virus signatures no less than once per day and (b) the related anti-virus signatures are current and no less recent than two versions/releases behind the most current version/release of the anti-virus signatures for the anti-virus software

(ii) Contractor shall provide for prompt application of security updates for operating systems used on all Contractor Managed Systems.

B. System Hardening

Contractor shall ensure unnecessary services and ports are disabled prior to implementation of this Agreement. Contractor must review and apply recommendations based on NIST's National Vulnerability Database, available at https://nvd.nist.gov/.

C. Authentication

(i) Contractor shall assign a unique user ID to any Contractor Personnel or County end user who accesses County Data on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

(ii) Unless otherwise agreed by County, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

D. Data Protection

County shall implement processes and/or controls to prevent the accidental disclosure of County Data to other customers of Contractor.

E. Account Termination

Contractor shall disable user accounts of any personnel who access the system provided under the Contract within one (1) business day of becoming aware of the termination of such individual. In the cases of termination for cause, Contractor will disable such user accounts as soon as administratively possible and no later than one (1) business days.

F. System/Data Access

(i) Contractor and Contractor Personnel shall only access County and Contractor Managed Systems, applications, or County Data for which they are expressly authorized by County to access, even if the technical controls in the system or application do not prevent Contractor or Contractor Personnel from accessing those data or functions outside of County's authorization. Contractor shall impose reasonable sanctions against any of Contractor Personnel who attempt to bypass security controls.

(ii) Contractor agrees to use the principle of least privilege when granting access to Contractor Managed Systems or County Data.

G. System Maintenance

Contractor shall maintain system(s) that generate, store, transmit or process County Data according to manufacturer recommendations. Contractor shall ensure that only those Contractor Personnel certified to repair such systems are allowed to provide maintenance services.

11. Software / System Capability

A. Supported Product

(i) Unless otherwise expressly agreed by County in writing, Contractor shall provide County only supported versions of the Product, which will not become "end of life" for at least 24 months. When the Product or Service provided pursuant to this Agreement requires third party components, Contractor must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by County, Contractor represents that all third-party components in its Product are currently supported, are not considered "end of life" by the third-party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by County.

(ii) If open source software is incorporated into the Product, Contractor shall only use widely supported and active open source software in the Product and shall disclose such software to County prior to its acquisition of the Product.

B. Software Capabilities Requirements

(i) Contractor's Product shall support a configurable session timeout for all users or administrative access to the Product.

(ii) Contractor shall ensure that Products provided can be configured to require a Strong Password for user authentication.

(iii) Contractor's Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.

C. Backdoor Software. Contractor shall not provide Products with backdoor software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Contractor shall supply all information needed for the County to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Contractor. Contractor shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

D. Remote Access Software. Contractor shall not provide Products that will allow for Remote Access from untrusted networks by default.

EXHIBIT E

COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES

1. DEFINITIONS

(a) *"Users"* include all employees, agents and/or representatives of Contractor performing services under this Agreement.

(b) *"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

(c) *"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.

(d) "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.

(e) *"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.

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 Attachment A. 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 County 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 this Agreement. Users must be aware of security issues and shall immediately report incidents to County 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.

(n) 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) User 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.

(o) 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.

(p) 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.

(q) 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.

(r) 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. Contractor shall configure all Contractor-provided computer devices authorized by the County and 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. County will first confer with Contractor on feasibility of any additional security-related system configurations or software to ensure Contractor's ability to provide remote access support.

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 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.

e. Users 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 County within 24 hours.

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. County shall work with and allow Contractor Users to configure Contractor-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. User 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. User 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. User 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. User shall report to County within 24 hours any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the third-party owned device, including loss or theft of the device.

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: Date Signed:

Print User Name:

EXHIBIT F

VENDOR REMOTE ACCESS AGREEMENT

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:

Automated Fingerprint Identification System (AFIS)

Automated Fingerprint Identification System Disaster Recovery (AFIS-DR)

LiveScan

(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: Gordon Warden

County: Tim Fayle

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.

(iv) 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.

EXHIBIT G

PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

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

. Santa Clara County Sheriff's Office (Public law enforcement/criminal justice agency)

CA0430000 (ORI)

to Idemia Identity & Security USA LLC (Private Contractor)

to perform maintenance & support of automated fingerprint identification system (AFIS) and County Live Scans Services on its behalf. (Type of service)

Access to the CLETS is authorized to public law enforcement and criminal justice agencies only (hereinafter referred to as the *CLETS subscribing agency),* 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, nor 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 FBI's *CJ/S 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 the CLETS systems access to personnel who meet these standards and deny it to those who do not; and
2. Policies governing the operation of computers, access devices, circuits, hubs, ***boundary protection devices*** 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 terminals, access devices or stored/printed data.

Additionally, it is the responsibility of the CLETS subscribing agency to ensure 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 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 retesting and reaffirm the proficiency of all the CLETS operators, ifapplicable;
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 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; and
3. Each individual must sign an Employee Volunteer Statement Form prior to operating or having access to the CLETS computers, equipment or information.

In accordance with the CLETS/NCIC policies, the CLET.S 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 Management Control Agreement 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; using, disseminating 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)	Signature (private contractor)
Print Name and Title	Print Name and Title
Date	Date

Approved as to form and legality
Tara Lundstrom
Tara Lundstrom, Deputy County Counsel
Office of the County Counsel
Date 6/24/2019

EXHIBIT G-1

CLETS EMPLOYEE/VOLUNTEER STATEMENT

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

As an employee/volunteer of_____, 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.

_____ _____

Signature Print Name

_____

Date

EXHIBIT H

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

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

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

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The

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

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

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

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

   1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

   2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

   3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain

such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

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

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

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

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

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

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

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

1.00 Definitions

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

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

2.00 Responsibilities of the Contracting Government Agency.

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

3.00 Responsibilities of the Contractor.

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

4.00 Security Violations.

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

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

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

5.00 Audit

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

6.00 Scope and Authority

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

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

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

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

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

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 limitedto, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

EXHIBIT I-1

BIOMETRIC PRODUCTS AND SYSTEM SALES AGREEMENT

Idemia Identity & Security USA LLC
Biometrics Products and System Sales Agreement
Idemia Identity & Security USA LLC may be referred to as "IDEMIA" or "Seller" and County of Santa Clara may be referred to as "County" or "Customer".

SECTION 1. EXHIBITS
Intentionally omitted.

SECTION 2. DEFINITIONS
Capitalized terms used in this Exhibit shall have the following meanings:

2.1 Intentionally Omitted.

2.2 "Contract Price" means the price for the System or Products, exclusive of any applicable sales or similar taxes and freight charges.

2.3 "Effective Date" means that date upon which the last party to sign this Agreement has executed it.

2.4 "Equipment" means the equipment listed in the List of Deliverables or List of Products that Customer is purchasing from Seller under this Agreement.

2.5 "Infringement Claim" means a third party claim alleging that the Equipment manufactured by IDEMIA or the IDEMIA Software infringes upon the third party's United States patent or copyright.

2.6 "IDEMIA" means IDEMIA Identity & Security USA LLC, a Delaware limited liability company.

2.7 "IDEMIA Software" means Software that IDEMIA or Seller owns.

2.8 "Non-IDEMIA Software" means Software that a party other than IDEMIA or Seller owns.

2.9 "Open Source Software" means software that has its underlying source code freely available to evaluate, copy, and modify. Open Source Software and the terms "freeware" or "shareware" are sometimes used interchangeably.

2.11 "Products" means the Equipment and Software provided by Seller under this Agreement.

2.12 "Proprietary Rights" means the patents, patent applications, inventions, copyrights, trade secrets, trademarks, trade names, mask works, know-how, and other intellectual property rights in and to the Equipment and Software, including those created or produced by IDEMIA or Seller under this Agreement and any corrections, bug fixes, enhancements, updates or modifications to or derivative works from the Software whether made by IDEMIA or another party.

2.13 "Software" means the IDEMIA Software and Non-IDEMIA Software in object code format that is furnished with the System or Equipment and which may be listed on the List of Deliverables or List of Products.

2.14 "Specifications" means the functionality and performance requirements described in the Technical and Implementation Documents.

2.15 "Subsystem" means a major portion of the entire System that performs specific functions or operations as described in the Technical and Implementation Documents.

2.16 "System" means the Equipment, Software, services, supplies, and incidental hardware and materials combined together into a system as more fully described in the Technical and Implementation Documents.

2.17 "System Acceptance" means the Acceptance Tests have been successfully completed.

2.18 Technical and Implementation Documents means the written technical detailed documentation(s) of the functional and performance requirements for the System(s) and/or Subsystem(s), such as a requirements definition document, and/or interface control document, and/or data dictionary, and/or system design document.

SECTION 3. SCOPE OF AGREEMENT AND TERM

3.1. SCOPE OF WORK. For System sales, Seller will provide, ship, install and test the System, and perform its other contractual responsibilities, all in accordance with this Agreement. Customer will perform its contractual responsibilities in accordance with this Agreement. For Product sales, Seller will provide, ship, and install (if applicable) the Products, and perform its other contractual responsibilities, all in accordance with this Agreement. Customer will perform its contractual responsibilities in accordance with this Agreement.

3.5. MAINTENANCE SERVICE.

3.5.1. System Sales. After the warranty period, Customer may purchase maintenance and support services for the Equipment and IDEMIA Software by executing an extended Maintenance and Support Agreement.

3.5.2. Product Sales. This Agreement does not cover maintenance or support of the Products except as provided under the warranty. If Customer wishes to purchase maintenance or support, Seller will provide a separate maintenance and support proposal upon request.

3.6. IDEMIA SOFTWARE. Any IDEMIA Software, including subsequent releases, is licensed to Customer solely in accordance with the Software License Agreement. Customer hereby accepts and agrees to abide by all of the terms and restrictions of the Software License Agreement.

3.7. NON-IDEMIA SOFTWARE. Any Non-IDEMIA Software is licensed to Customer in accordance with the standard license, terms, and restrictions of the copyright owner on the Effective Date unless the copyright owner has granted to IDEMIA the right to sublicense the Non-IDEMIA Software pursuant to the Software License Agreement, in which case it applies and the copyright owner will have all of Licensor's rights and protections under the Software License Agreement. IDEMIA makes no representations or warranties of any kind regarding Non-IDEMIA Software. Non-IDEMIA Software may include Open Source Software. All Open Source Software is licensed to Customer in accordance with, and Customer agrees to abide by, the provisions of the standard license of the copyright owner and not the Software License Agreement. Upon request by Customer, IDEMIA will use commercially reasonable efforts to (i) determine whether any Open Source Software will be provided under this Agreement; and if so, (ii) identify the Open Source Software and provide to Customer a copy of the applicable standard license (or specify where such license may be found); and (iii) provide to Customer a copy of the Open Source Software source code if it is publicly available without charge (although a distribution fee or a charge for related services may be applicable).

3.8. SUBSTITUTIONS. At no additional cost to Customer, Seller reserves the right to substitute any Equipment, Software, or services to be provided by Seller, provided that the substitute meets or exceeds the Specifications and is of equivalent or better quality to the Customer. Any such substitution will be reflected in a change order.

3.9. OPTIONAL EQUIPMENT OR SOFTWARE. This paragraph applies only if a "Priced Options" exhibit is shown in Section 1 of this Agreement, or if the Parties amend this Agreement to add a Priced Options exhibit. During the term of the option as stated in the Priced Options exhibit (or if no term is stated, then for one (1) year after the Effective Date), Customer shall have the right and option to purchase the equipment, software, and related services that are described and listed in the Priced Options exhibit. Customer may exercise this option by giving written notice to Seller which must designate what equipment, software, and related services Customer is selecting (including quantities, if applicable). To the extent they apply, the terms and conditions of this Agreement will govern the purchase of the selected equipment, software, and related services. However, the parties acknowledge that certain contractual provisions must be agreed upon, and they agree to negotiate those in good faith promptly after Customer delivers to Seller the option exercise notice. Examples of provisions that may need to be negotiated are: specific lists of deliverables, statements of work, acceptance test plans, delivery and implementation schedules, payment terms, maintenance and support provisions, additions to or modifications of the Software License Agreement, hosting terms, and modifications to the acceptance and warranty provisions.

SECTION 4. PERFORMANCE SCHEDULE
INTENTIONALLY OMITTED

SECTION 5. CONTRACT PRICE, PAYMENT, AND INVOICING
INTENTIONALLY OMITTED

SECTION 6. SITES AND SITE CONDITIONS

6.1. ACCESS TO SITES. In addition to its responsibilities described elsewhere in this Agreement, Customer will provide (i) a designated project manager; (ii) all necessary construction and building permits, zoning variances, licenses, and any other approvals that are necessary to develop or use the sites; and (iii) access to the work sites identified in the Technical and Implementation Documents as reasonably requested by Seller so that it may perform its duties in accordance with the Performance Schedule and Statement of Work.

6.2. SITE CONDITIONS. Customer will ensure that all work sites it provides will be safe, secure, and in compliance with all applicable industry and OSHA standards. To the extent applicable and unless the Statement of Work specifically states to the contrary, Customer will ensure that these work sites will have (i) adequate physical space for the installation, use and maintenance of the System; (ii) adequate air conditioning and other environmental conditions; (iii) adequate electrical power outlets, distribution and equipment for the installation, use and maintenance of the System; and (iv) adequate telephone or other communication lines for the installation, use and maintenance of the System, including modem access, and adequate interfacing networking capabilities. Before installing the Equipment or Software at a work site, Seller will inspect the work site and advise Customer of any apparent deficiencies or non-conformities with the requirements of this Section.

6.3. SITE ISSUES. If Seller or Customer determines that the sites identified in the Technical and Implementation Documents are no longer available or desired, or if subsurface, structural, adverse environmental or latent conditions at any site differ from those indicated in the Technical and Implementation Documents, Seller and Customer will promptly investigate the conditions and will select replacement sites or adjust the installation plans and Specifications as necessary. If such change in sites or adjustment to the installation plans and Specifications causes a change in the cost or time to perform, the parties will equitably amend the Contract Price or Performance Schedule, or both, by a change order.

SECTION 7. TRAINING
Intentionally omitted.

SECTION 8. ACCEPTANCE
Intentionally omitted.

8.2 PRODUCT ACCEPTANCE

8.2.1. Acceptance of the Products will occur upon delivery to Customer unless the Statement of Work provides for acceptance verification or testing, in which case acceptance of the Products will occur upon successful completion of the acceptance verification or testing. Notwithstanding the preceding sentence, Customer's use of the Products for their operational purposes will constitute acceptance.

SECTION 9. REPRESENTATIONS AND WARRANTIES

9.1. SYSTEM FUNCTIONALITY (System sales only). Seller represents that the System will perform in accordance with the Specifications in all material respects. Upon System Acceptance or Beneficial Use, whichever occurs first, this System functionality representation is fulfilled. Seller is not responsible for System performance deficiencies that are caused by ancillary equipment not furnished by Seller attached to or used in connection with the System or for reasons beyond Seller's control, such as (i) an earthquake, adverse atmospheric conditions, or other natural causes; (ii) Customer changes to load usage or configuration outside the Specifications; or (iii) any acts of parties who are beyond Seller's control.

9.2. EQUIPMENT WARRANTY.

9.2.1. System Sales For one (1) year from the date of System Acceptance or Beneficial Use, whichever occurs first, Seller warrants that the Equipment under normal use and service will be free from material defects in materials and workmanship and meet the requirements set forth in this Agreement. If System Acceptance is delayed beyond six (6) months after shipment of the Equipment by events or causes within Customer's control, this warranty expires eighteen (18) months after the shipment of the Equipment.

9.2.2. Product Sales For one (1) year from the date of shipment, Seller warrants that the Equipment under normal use and service will be free from material defects in materials and workmanship and meet the requirements set forth in this Agreement.

9.3. IDEMIA SOFTWARE WARRANTY.

9.3.1 System Sales Unless otherwise stated in the Software License Agreement, for one (1) year from the date of System Acceptance or Beneficial Use, whichever occurs first, Seller warrants the IDEMIA Software in accordance with the terms of the Software License Agreement and the provisions of this Section 9 that are applicable to the IDEMIA Software and will meet the requirements set forth in this Agreement. If System Acceptance is delayed beyond six (6) months after shipment of the IDEMIA Software by events or causes within Customer's control, this warranty expires eighteen (18) months after the shipment of the IDEMIA Software.

9.3.2. Product Sales Unless otherwise stated in the Software License Agreement, for one (1) year from the date of shipment, Seller warrants the IDEMIA Software in accordance with the terms of the Software License Agreement and the provisions of this Section that are applicable to the IDEMIA Software and will meet the requirements set forth in this Agreement.

9.4. EXCLUSIONS TO EQUIPMENT AND IDEMIA SOFTWARE WARRANTIES. These warranties do not apply to: (i) defects or damage resulting from use of the Equipment or IDEMIA Software in other than its normal, customary, and authorized manner; (ii) defects or damage occurring from misuse, accident, liquids, neglect, or acts of God; (iii) defects or damage occurring from testing, maintenance, disassembly, repair, installation, alteration, modification, or adjustment not provided or authorized in writing by Seller; (iv) breakage of or damage to antennas unless caused directly by defects in material or workmanship; (v) defects or damage caused by Customer's failure to comply with all applicable industry and OSHA standards; (vi) Equipment that has had the serial number removed or made illegible; (vii) batteries (because they carry their own separate limited warranty); (viii) freight costs to ship Equipment to the repair depot; (ix) scratches or other cosmetic damage to Equipment surfaces that does not affect the operation of the Equipment; and (x) normal or customary wear and tear.

9.5. WARRANTY CLAIMS. For Customer to assert a claim that the Equipment or IDEMIA Software does not conform to these warranties, Customer must notify Seller in writing of the claim before the expiration of the warranty period. Upon receipt of such notice, Seller will investigate the warranty claim. If this investigation confirms a valid warranty claim, Seller will (at its option and at no additional charge to Customer) repair the defective Equipment or IDEMIA Software, replace it with the same or equivalent product, or refund the price of the defective Equipment or IDEMIA Software. Such action will be the full extent of Seller's liability hereunder. Repaired or replaced product is warranted for the balance of the original applicable warranty period. All replaced products or parts will become the property of Seller.

9.6. ORIGINAL END USER IS COVERED. These express limited warranties are extended by Seller to the original user purchasing the System or Products for commercial, industrial, or governmental use only, and are not assignable or transferable.

9.7. DISCLAIMER OF OTHER WARRANTIES. THESE WARRANTIES ARE THE COMPLETE WARRANTIES FOR THE EQUIPMENT AND IDEMIA SOFTWARE PROVIDED UNDER THIS AGREEMENT AND ARE GIVEN IN LIEU OF ALL OTHER WARRANTIES. SELLER DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

SECTION 10. DELAYS
Intentionally Omitted

10.2. PERFORMANCE SCHEDULE DELAYS CAUSED BY CUSTOMER (System Sales Only). If the Performance Schedule is delayed solely because of Customer (including any of its other contractors), (i) Customer will make the promised payments according to the Payment Schedule as if no delay occurred; and (ii) the parties will execute a change order to extend the Performance Schedule and, if requested by Seller, compensate Seller for all reasonable charges incurred because of such delay. Delay charges may include costs incurred by Seller or its subcontractors for additional freight, warehousing and handling of Equipment; extension of the warranties; travel; suspending and re-mobilizing the work; additional engineering, project management, and standby time calculated at then current rates; and preparing and implementing an alternative implementation plan.

SECTION 11. DISPUTES
INTENTIONALLY OMITTED

SECTION 12. DEFAULT AND TERMINATION
INTENTIONALLY OMITTED

SECTION 14. LIMITATION OF LIABILITY

This limitation of liability provision shall apply notwithstanding any contrary provision in this Agreement. Except for personal injury or death, each party's total liability to the other party, whether for breach of contract, warranty, negligence, strict liability in tort, indemnification, or otherwise, will be limited to the direct damages recoverable under law, but not to exceed the price of the Equipment, Software, or services with respect to which losses or damages are claimed. ALTHOUGH THE PARTIES ACKNOWLEDGE THE POSSIBILITY OF SUCH LOSSES OR DAMAGES, THEY AGREE THAT A PARTY WILL NOT be liable for any commercial loss; inconvenience; loss of use, time, data, goodwill, revenues, profits or savings; or other SPECIAL, incidental, INDIRECT, OR consequential damages IN ANY WAY RELATED TO OR ARISING FROM THIS AGREEMENT, THE SALE OR USE OF THE EQUIPMENT OR SOFTWARE, OR THE PERFORMANCE OF SERVICES BY SELLER PURSUANT TO THIS AGREEMENT. This limitation of liability will survive the expiration or termination of this Agreement. This section shall not apply to fraud, gross negligence, willful misconduct, indemnity obligations in the Agreement, privacy breaches or security breaches.

SECTION 15. CONFIDENTIALITY AND PROPRIETARY RIGHTS

15.1. CONFIDENTIAL INFORMATION.

15.1.1. During the term of this Agreement, the parties may provide each other with Confidential Information. For the purposes of this Agreement, "Confidential Information" is any information disclosed in written, graphic, verbal, or machine-recognizable form, and is marked, designated, labeled or identified at the time of disclosure as being confidential or its equivalent; or if in verbal form is identified as confidential or proprietary at the time of disclosure and confirmed in writing within thirty (30) days of such disclosure. Notwithstanding any other provisions of this Agreement, Confidential Information shall not include any information that: (i) is or becomes publicly known through no wrongful act of the receiving party; (ii) is already known to the receiving party without restriction when it is disclosed; (iii) is, or subsequently becomes, rightfully and without breach of this Agreement, in the receiving party's possession without any obligation restricting disclosure; (iv) is independently developed by the receiving party without breach of this Agreement; or (v) is explicitly approved for release by written authorization of the disclosing party.

15.1.2. Subject to the California Public Records Act and Section 43 of the Agreement, each party will: (i) maintain the confidentiality of the other party's Confidential Information and not disclose it to any third party, except as authorized by the disclosing party in writing or as required by a court of competent jurisdiction; (ii) restrict disclosure of Confidential Information to its employees who have a "need to know" and not copy or reproduce such Confidential Information; (iii) take necessary and appropriate precautions to guard the confidentiality of Confidential Information, including informing its employees who handle such Confidential Information that it is confidential and not to be disclosed to others, but such precautions shall be at least the same degree of care that the receiving party applies to its own confidential information and shall not be less than reasonable care; and (iv) use such Confidential Information only in furtherance of the performance of this Agreement. Confidential Information is and shall at all times remain the property of the disclosing party, and no grant of any proprietary rights in the Confidential Information is hereby given or intended, including any express or implied license, other than the limited right of the recipient to use the Confidential Information in the manner and to the extent permitted by this Agreement.

15.2. PRESERVATION OF PROPRIETARY RIGHTS.

15.2.1. IDEMIA, the third party manufacturer of any Equipment, and the copyright owner of any Non-IDEMIA Software own and retain all of their respective Proprietary Rights in the Equipment and Software. Nothing in this Agreement is intended to restrict the Proprietary Rights of IDEMIA, any copyright owner of Non-IDEMIA Software, or any third party manufacturer of Equipment. All intellectual property developed, originated, or prepared by IDEMIA in connection with providing to Customer the Equipment, Software, or related services remain vested exclusively in IDEMIA, and this Agreement does not grant to Customer any shared development rights of intellectual property.

15.2.2. Except as explicitly provided in the Software License Agreement, nothing in this Agreement will be deemed to grant, either directly or by implication, estoppel, or otherwise, any right, title or interest in the Proprietary Rights of IDEMIA or Seller. Customer agrees not to modify, disassemble, peel components, decompile, otherwise reverse engineer or attempt to reverse engineer, derive source code or create derivative works from, adapt, translate, merge with other software, reproduce, or export the Software, or permit or encourage any third party to do so. The preceding sentence shall not apply to Open Source Software which is governed by the standard license of the copyright owner.

Exhibit I-2 - Software License Agreement

EXHIBIT I-2 - SOFTWARE LICENSE AGREEMENT

In this Exhibit I-2, the term "Licensor" means IDEMIA Identity & Security USA LLC, ("IDEMIA"); "Licensee," means the County or Customer; "Agreement" means the agreement to which this exhibit is attached; and "SLA" means this Exhibit and the applicable terms and conditions contained in the Agreement. The parties agree as follows:

For good and valuable consideration, the parties agree as follows:

SECTION 1. DEFINITIONS

1.1 "Designated Products" means products provided by IDEMIA to Licensee with which or for which the Software and Documentation is licensed for use.

1.2 "Documentation" means product and software documentation that specifies technical and performance features and capabilities, and the user, operation and training manuals for the Software (including all physical or electronic media upon which such information is provided).

1.3 "Open Source Software" means software with either freely obtainable source code, license for modification, or permission for free distribution.

1.4 "Open Source Software License" means the terms or conditions under which the Open Source Software is licensed.

1.6 "Security Vulnerability" means a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach such that data is compromised, manipulated or stolen or the system damaged.

1.7 "Software" (i) means proprietary software in object code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by IDEMIA; and (iii) may contain one or more items of software owned by a third party supplier. The term "Software" does not include any third party software provided under separate license or third party software not licensable under the terms of this Agreement.

SECTION 2. SCOPE

IDEMIA and Licensee enter into this SLA in connection with IDEMIA's delivery of certain proprietary Software or products containing embedded or pre-loaded proprietary Software, or both. This SLA contains the terms and conditions of the license IDEMIA is providing to Licensee, and Licensee's use of the Software and Documentation.

SECTION 3. GRANT OF LICENSE

3.1. Subject to the provisions of this SLA and the payment of applicable license fees, IDEMIA grants to Licensee a personal, limited, non-transferable (except as permitted in Section 7) and non-exclusive license under IDEMIA's copyrights and Confidential Information (as defined in the Primary Agreement) embodied in the Software to use the Software, in object code form, and the Documentation solely in connection with Licensee's use of the Designated Products. This SLA does not grant any rights to source code.

3.2. If the Software licensed under this SLA contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the Open Source Software Licenses governing Licensee's use of the Open Source Software, the terms and conditions of the license grant of the applicable Open Source Software Licenses will take precedence over the license grants in this SLA. If requested by Licensee, IDEMIA will use commercially reasonable efforts to: (i) determine whether any Open Source Software is provided under this SLA; (ii) identify the Open Source Software and provide Licensee a copy of the applicable Open Source Software License (or specify where that license may be found); and, (iii) provide Licensee a copy of the Open Source Software source code, without charge, if it is publicly available (although distribution fees may be applicable).

SECTION 4. LIMITATIONS ON USE

4.1. Licensee may use the Software only for Licensee's internal business purposes and only (which includes fulfilling its mission of providing services to the public) in accordance with the Documentation. Any other use of the Software is strictly prohibited. Without limiting the general nature of these restrictions, Licensee will not make the Software available for use by third parties on a "time sharing," "application service provider," or "service bureau" basis or for any other similar commercial rental or sharing arrangement.

4.2. Licensee will not, and will not allow or enable any third party to: (i) reverse engineer, disassemble, peel components, decompile, reprogram or otherwise reduce the Software or any portion to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party, grant any sublicense or other rights in the Software or Documentation to any third party, or take any action that would cause the Software or Documentation to be placed in the public domain; (iv) remove, or in any way alter or obscure, any copyright notice or other notice of IDEMIA's proprietary rights; (v) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by any third party or on any machine except as expressly authorized by this Agreement; or (vi) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software solely by activating a machine containing the Software. Licensee may make one copy of Software to be used solely for archival, back-up, or disaster recovery purposes; provided that Licensee may not operate that copy of the Software at the same time as the original Software is being operated. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.

4.3. Unless otherwise authorized by IDEMIA in writing, Licensee will not, and will not enable or allow any third party to: (i) install a licensed copy of the Software on more than one unit of a Designated Product; or (ii) copy onto or transfer Software installed in one unit of a Designated Product onto another device. Licensee may temporarily transfer Software installed on a Designated Product to another device if the Designated Product is inoperable or malfunctioning, if Licensee provides written notice to IDEMIA of the temporary transfer and identifies the device on which the Software is transferred. Temporary transfer of the Software to another device must be discontinued when the original Designated Product is returned to operation and the Software must be removed from the other device. Licensee must provide prompt written notice to IDEMIA at the time temporary transfer is discontinued.

SECTION 5. OWNERSHIP AND TITLE

IDEMIA, its licensors, and its suppliers retain all of their proprietary rights in any form in and to the Software and Documentation, including, but not limited to, all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, emulations to or derivative works from the Software or Documentation, whether made by IDEMIA or another party, or any improvements that result from IDEMIA's processes or, provision of information services).

No rights are granted to Licensee under this SLA by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Agreement. All intellectual property developed, originated, or prepared by IDEMIA in connection with providing the Software, Designated Products, Documentation or related services, remains vested exclusively in IDEMIA, and Licensee will not have any shared development or other intellectual property rights.

SECTION 6. LIMITED WARRANTY; DISCLAIMER OF WARRANTY

6.1. If Licensee is not in breach of any of its obligations under this SLA, IDEMIA warrants that the unmodified Software, when used properly and in accordance with the Documentation and this SLA, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect occurs will be determined by IDEMIA solely with reference to the Documentation. IDEMIA does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. IDEMIA makes no representations or warranties with respect to any third party software included in the Software.

6.2 IDEMIA's sole obligation to Licensee and Licensee's exclusive remedy under this warranty is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant, demonstrable program or documentation errors or Security Vulnerabilities. If IDEMIA cannot correct the defect within a reasonable time, then at IDEMIA's option, IDEMIA will replace the defective Software with functionally-equivalent Software, license to Licensee substitute Software which will accomplish the same objective, or terminate the license and refund the Licensee's paid license fee.

6.3. Warranty claims are described in the Agreement.

6.4. The express warranties set forth in this Section 6 are in lieu of, and IDEMIA disclaims, any and all other warranties (express or implied, oral or written) with respect to the Software or Documentation, including, without limitation, any and all implied warranties of condition, title, non-infringement, merchantability, or fitness for a particular purpose or use by Licensee (whether or not IDEMIA knows, has reason to know, has been advised, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, IDEMIA disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

SECTION 7. TRANSFERS
Licensee will not transfer the Software or Documentation to any third party without IDEMIA's prior written consent. IDEMIA's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this SLA.

SECTION 8. TERM AND TERMINATION
8.1 Licensee's right to use the Software and Documentation will begin when the Agreement is signed by both parties and will continue for the life of the Designated Products with which or for which the Software and Documentation have been provided by IDEMIA, unless Licensee breaches this SLA, in which case this SLA and Licensee's right to use the Software and Documentation may be terminated if not cured by Licensee within thirty (30) days of notice by IDEMIA.

8.2 Within thirty (30) days after termination of this Agreement, Licensee must certify in writing to IDEMIA that all copies of the Software have been removed or deleted from the Designated Products and that all copies of the Software and Documentation have been returned to IDEMIA or destroyed by Licensee and are no longer in use by Licensee.

8.3 Licensee acknowledges that IDEMIA made a considerable investment of resources in the development, marketing, and distribution of the Software and Documentation and that Licensee's breach of this SLA will result in irreparable harm to IDEMIA for which monetary damages would be inadequate. If Licensee breaches this Agreement, IDEMIA may terminate this SLA and be entitled to all available remedies at law or in equity (including immediate injunctive relief and repossession of all non-embedded Software and associated Documentation unless Licensee is a Federal agency of the United States Government).

SECTION 9. UNITED STATES GOVERNMENT LICENSING PROVISIONS & RESTRICTED RIGHTS LEGEND
Intentionally omitted because Licensee is not the United States Government or a United States Government agency.

SECTION 10. CONFIDENTIALITY
Licensee acknowledges that the Software and Documentation contain IDEMIA's valuable proprietary and Confidential Information and are IDEMIA's trade secrets, and that the provisions in the Agreement concerning Confidential Information apply.

SECTION 11. GENERAL
11.1. COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.