EXHIBIT B

SERVICE LEVEL AGREEMENT

TABLE OF CONTENTS

1.0 GENERAL

This Exhibit B, Service Level Agreement (hereinafter SLA), sets forth the scope of, and Contractor's Service level commitment regarding the Maintenance and Support Services (M&S) for the ICSS, including but not limited to, M&S service levels for Hardware and Software support, correction of Deficiencies, warranties, and the County's remedies for Contractor's failure to meet the Service level commitment specified herein. This SLA is supplemental to the warranties and representations made in the Contract. Capitalized terms used in this SLA without definition will have the meanings given to such terms in the Contract.

2.0 SCOPE OF SERVICES

2.1 Description

Contractor must provide M&S services as specified in the Contract, Exhibit A (Statement of Work) and this SLA, as more fully described in Paragraph 2.2 (Definitions) below.

2.2 Definitions

Deficiency Credits: Credits (or any other form of discount) to be applied to the applicable Service fees for Contractor's failure to resolve an Incident, or correct a Deficiency, including ICSS Downtime.

Downtime: The period of time that the ICSS cannot be accessed due to any component of the ICSS being inaccessible. This excludes any scheduled Downtime that has been mutually agreed to by both parties.

Incident: A circumstance or set of circumstances taken together, resulting in a failure to meet a Service level as required under Exhibit A (Statement of Work) and this SLA, and which can result in a Downtime credit.

Maintenance Services: Any goods or Services provided under the Contract for maintaining the ICSS. This includes, but is not limited to:

a. Hardware Maintenance (e.g., Preventive Maintenance, and scheduled/ unscheduled equipment repairs or replacement), and

b. Software Maintenance [e.g., Preventive Maintenance, software upgrades, updates, enhancements, patches, and other updates to the ICSS software needed to maintain compatibility with the ICCS, software security updates, and report design updates, as further outlined in Paragraph 3.0 (Maintenance Services) of this SLA.]

Preventive Maintenance: The regular inspection, cleaning, and replacement of ICSS components in order to optimize ICSS functionality and prevent any unscheduled Downtime due to ICSS failure.

Severity Level: The applicable Deficiency severity level assigned to each Incident, for purposes of correcting Deficiencies, as described in Paragraph 4.2 (Resolution of Deficiencies) of this SLA.

Support Hours: Means 365/366 Days per year, 24 hours per Day, 7 Days per week, with no exceptions made for holidays.

Support Services: Contractor's provision to the County of customer support services and Technical Support Center, as applicable.

Technical Support Center: Has the meaning described in Paragraph 3.4 (Contractor's 24/7 Technical Support Center) of this SLA.

3.0 MAINTENANCE SERVICES

3.1 As part of ICSS maintenance, Contractor must provide Maintenance Services for all ICSS hardware and software delivered by Contractor to the County, as applicable, all as part of the ICSS (hereinafter "Maintenance Services"), as provided herein.

3.1.1 Any ICSS solution maintenance must be coordinated not less than 72 hours in advance and approved by the County.

3.2 Contractor must ensure the ICSS is available 24/7 and must maintain ICSS availability at a minimum of 99.5% of the time except for approved scheduled ICSS maintenance [refer to Paragraph 3.6 (System Hardware Maintenance) of this SLA].

Notwithstanding the above, the County, in its sole discretion, may shut down Inmate Telephone Instruments, during normal business operations, for scheduled periods of time, such as mandatory Inmate counts, or during scheduled nighttime "lights out" hours.

3.3 Hours and Days of Service

As part of Contractor's M&S, Contractor must provide on-site technical staff to support the administration, operation, and maintenance of the ICSS at Facilities. Such activities are to be performed during the County's Normal Business Hours, excluding County-recognized holidays (list to be provided).

3.3.1 On-Call for Emergency Repairs

Contractor must provide on-call technical staff to respond to after-hours emergency repairs (i.e., Severity Levels 1 and 2 service requests) to the ICSS. Refer to the Response Times listed in Paragraph 4.3 (ICSS Response Times) of this SLA.

3.4 Contractor's 24/7 Technical Support Center

Contractor must utilize a remotely located Technical Support Center to monitor ICSS operations 24/7 at Facilities and assist in the troubleshooting and resolution of ICSS problems including, but not limited to, connectivity issues associated with System Administrative Consoles provided under the Contract and investigator remote access to the recording, playback, and other feature functionality, within the span of control of Contractor.

3.4.1 During Normal Business Hours, Contractor's Technical Support Center must monitor and report any observed technical problems

or abnormal conditions pertaining to the operation and maintenance of the ICSS to County Project Manager.

3.4.2 During hours outside of Normal Business Hours, Contractor's Technical Support Center must continue to monitor and report any observed technical problems or abnormal conditions pertaining to the operation and maintenance of the ICSS, and dispatch on-call maintenance support staff for the repair and maintenance of problems based on the Severity Level assigned and resolution time stated in Paragraph 4.3 (ICSS Response Times) of this SLA. Contractor's Technical Support Center may defer the repair of minor problems, consistent with procedures approved in writing by County Project Manager.

3.4.2.1 The County will assign the Severity Level, and a service ticket is to be documented and tracked by Contractor's Technical Support Center as required for ICSS.

3.4.3 All requests from Contractor to obtain firewall privileges or access to the network for the provision of remote support, must be approved by County Project Manager.

3.5 Preventive Maintenance

Contractor must develop procedures and schedules to conduct monthly Preventative Maintenance to ensure the County has 24/7 uninterrupted availability of the ICSS, including all equipment and Telephone Instruments included therein. The Preventive Maintenance program must include, but is not limited to:

a. All necessary labor, parts (new OEM), materials (new OEM), technical personnel, and transportation necessary.

b. Hardware Preventive Maintenance including, but not limited to: inspections, cleaning, testing and connectivity, etc.

c. Software Preventive Maintenance including, but not limited to software reviews, etc.

3.6 System Hardware Maintenance

As part of Maintenance Services, Contractor must provide maintenance of the ICSS's hardware infrastructure. Contractor must pass through to the County all equipment warranties provided by the original equipment manufacturers at the point of sale. Contractor must repair, upgrade/replace, or oversee the repair, upgrade or replacement of, all ICSS hardware components as needed throughout the entire term of the Contract to comply with the ICSS's requirements, and the warranties specified herein in this SLA, and throughout the Contract.

3.6.1 As part of Contractor's Hardware Maintenance services for all Contractor-provided ICSS hardware, Contractor must:

a. Inspect, clean, and test connectivity of all hardware including connectivity between all redundant server nodes,

b. Utilize automated monitoring tools to monitor server operations at all installed sites, and report all Deficiencies to the County,

c. Agree with the County regarding the Severity Level of each identified hardware Deficiency, and remedy the Deficiency in accordance with Paragraph 4.2 (Resolution of Deficiencies) of this SLA, and

d. Provide technical support to administer and operate all ICSS environments (e.g., production, training, testing, and business continuity).

3.7 Application Software

3.7.1 M&S must include: a) any ICSS updates, software upgrades, enhancements, revisions, new application version releases, improvements, bug fixes, security patches, and modifications to the ICSS or any component thereof, b) any testing or modifications necessary to maintain ICSS functionality, including any updates, and c) any upgrades or modifications required during the term to ensure the ICSS and each component thereof will remain in compliance with applicable federal or state and local laws and regulations (collectively, Updates hereinafter).

3.7.1.1 Contractor is responsible for the installation of security patches and appropriate software updates to all ITDs, servers, and workstations (if any) within 90 days of availability of such software.

3.7.1.2 Any ITD solution security patches, Updates, upgrades must be scheduled five days in advance and approved by the County.

3.7.2 Any update delivered by Contractor to the County will be deemed a part of the ICSS and must be included in the rights granted to the County pursuant to the Contract.

3.7.3 Without limiting the other provisions of the Contract including, without limitation, the provisions of this SLA, such Updates must be provided to the County at least once every year, unless otherwise agreed-to by the County and Contractor. Contractor must notify the County, at least two weeks in advance, of all such Updates to the Application Software prior to the anticipated installation date thereof. Contractor must test Updates in the test environment. The County will assess impacts to its business processes, if any, and verify whether the Updates were tested successfully. If so, Contractor must proceed with transitioning updates to the production environment. If not, Contractor must

conduct additional testing, until the County verifies successful testing.

3.7.4 Notwithstanding, the County may choose at its sole discretion to not implement a particular software update. Contractor and the County will discuss the impacts and risks to the County, if any, for not implementing a particular software update. Contractor must roll back any software Update to its prior version, as instructed by the County, when severe issues arise (as determined by both parties. Contractor must provide the County with a clearly defined configuration management plan (i.e., version control and source code control processes).

3.7.5 Contractor's provision and installation of software Updates are provided as part of Contractor's annual M&S service delivery and will be at no additional cost to the County.

3.7.6 Any updates necessary to remedy security problems in the ICSS (e.g., closing "back doors" or other intrusion-related problems) must be provided promptly following Contractor's knowledge of such problems. The County must also be notified in writing within no later than 24 hours of Contractor's knowledge of the existence of any intrusions or other security problems or breaches that may affect the integrity of the ICSS data or any other County data, subject to the provisions specified in Exhibit I (Information Security and Privacy Requirements) to the Contract.

3.8 Routine Maintenance and System Availability

Unless otherwise agreed to in advance by the County, Contractor must provide all Maintenance Services, including installation of Updates, with no Downtime. Any routine maintenance on a server or recording equipment that negatively impacts Telephone Instrument usage must be conducted by Contractor only during the hours of 12:01 a.m. and 6:00 a.m. (Pacific Time), Monday through Friday, and must include advance notification to the County via email, in-person, or by telephone during Normal Business Hours.

Contractor must notify County Project Directors and County Project Managers of any routine Downtime and as otherwise provided in this Paragraph 3.8 (Routine Maintenance and System Availability) via email, in-person, or by telephone during Normal Business Hours. If the routine Downtime will render inaccessible a component that provides recording or monitoring capabilities, then Contractor must provide County Project Manager at least 72 hours advance notice via email.

Any emergent Downtime will require immediate telephonic notification to County Project Manager.

If Downtime occurs, Paragraph 4.0 (Correction of Deficiencies) of this SLA will apply. In the event that ICSS maintenance is required, Contractor must ensure that, during any such ICSS maintenance, the ICSS availability

requirements of the Contract are met and that the ICSS remains fully operational.

3.9 Quality Assurance Inspections

Contractor must schedule and conduct monthly quality assurance inspections [refer to Paragraph 9.0 (Quality Assurance Plan) of the SOW], to ensure that Inmate Telephone Instruments at each of the Sheriff's and Probation Facilities are maintained in good working order. These monthly inspections must be documented in the Telephone Inspection and Maintenance Log Report [refer to Paragraph 7.3.1f (Telephone Inspection and Maintenance Log) of the SOW].

3.10 County Responsibilities

The County understands that in order for Contractor to provide M&S, the County:

a. Agrees that only authorized Sheriff Department or Probation Department employees (e.g., housing area officer reporting a Telephone Instrument not working, dorm officer reporting static on a phone line) will be authorized to request and receive M&S on behalf of the County (e.g., trouble ticket reporting).

b. Will provide Contractor with reasonable access to the ICSS during the times requested by Contractor, subject to the County Facility's access approval policies described in Paragraph 3.2 (Requirement's for Entry – Sheriff and Probation Facilities) of the SOW and otherwise in the Contract. Such access will be exclusively for M&S purposes and will be subject to Contractor's obligations to protect the County's proprietary and confidential information set forth in the Contract; and

c. Will provide Contractor with notice, either verbally or in writing, within three Days of a County known Deficiency occurrence being reported, with a general description of the Deficiency.

4.0 CORRECTION OF DEFICIENCIES

4.1 Identification of Deficiencies

Deficiencies may be identified either by Contractor's use of its own monitoring tools or discovered by the County. Upon discovery of a Deficiency by the County, the County will report the Deficiency and its Severity Level to Contractor's Technical Support Center for resolution in accordance with this SLA. Upon discovery of a Deficiency by Contractor, Contractor must report the Deficiency to County Project Manager. Regardless of the Deficiency discovery source, at all times, Contractor must keep the County informed on all identified Deficiencies. The parties must mutually agree to assign the appropriate Severity Level to any Deficiency discovered by Contractor.

The Severity Level of a Deficiency will be assigned according to the Severity Level definitions set forth in Paragraph 4.2.1 (Problem Correction Priorities) of this SLA. Based on Contractor's proposed solution and/or resolution time

for the Deficiency, the County may reevaluate, and escalate or downgrade the Severity Level of the Deficiency, pursuant to Paragraph 4.3.4 (Severity Level Adjustment) of this SLA.

4.2 Resolution of Deficiencies

4.2.1 Problem Correction Priorities

For each Deficiency reported by the County to Contractor, the County will assign the Severity Level to that Deficiency. For each Deficiency discovered by Contractor by its own problem monitoring the ICSS, Contractor will initially assign that Deficiency's Severity Level in consultation with the County.

Following a report of a Deficiency from the County, Contractor must respond back to the County within the prescribed "Service Response Timeframe" and resolve each such Deficiency within the specified "Service Resolution Time" as specified in the table below.

Following the report of a Deficiency by Contractor, Contractor must resolve each such Deficiency within the specified "Resolution Time" based on the Severity Level agreed-to by the parties.

Resolution times for correction of Deficiencies reported by the County will start tolling when the County first notifies Contractor of a Deficiency by telephone or as otherwise specified herein, including Contractor's Customer support, and will end when the County determines that the Deficiency has been resolved.

Conversely, resolution times for correction of Deficiencies reported by Contractor to the County will start tolling when Contractor should have notified or first notifies the County of a Deficiency by telephone or as otherwise specified herein, including Contractor's Customer support, and will end when the County determines that the Deficiency has been resolved.

4.3 ICSS Response Times

4.3.1 Inmate Telephone System – Response Times for Functionalities other than Monitoring

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
1 Critical	When 25% or more of a single housing unit's (Module/Dorm/Pod or Facility) Telephone Instruments are out of service.	Two Hours Credits applied for each hour thereafter an 'Incident'	Four Hours Credits double for all hours thereafter.

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
2 Severe	Up to 24% of a single housing unit's (Module/Dorm/Pod or Facility) Telephone Instruments are out of service. Or, when a single Telephone Instrument is out of service and more than five Inmates are not able to make telephone calls as a result.	Four Hours Credits applied for each hour thereafter an 'Incident'	Eight Hours Credits double for all hours thereafter.
3 Minor	When one Telephone Instrument is out of service but additional Telephone Instruments in the area are available for Inmates to use. System Administrative Console exhibits intermittent issues but is still operational.	Eight Hours Credits applied for each hour thereafter an 'Incident'	24 Hours Credits commence on hour thereafter.
4 Cosmetic	A Telephone Instrument is damaged but is capable of completing telephone calls.	24 Hours Credits applied for each hour thereafter an 'Incident'	Resolve Incident within three Business Days. Credits commence on Day 4 for each Day thereafter, 8am-5pm. Each Day thereafter an 'Incident'.

4.3.2 Inmate Telephone System – Response Times for Monitoring Functionalities

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
1 Critical	Recording or monitoring capabilities have stopped / or retrieval of recorded telephone calls cannot be accomplished, or the Contractor's supplied System Administrative Console will not function.	Two Hours Credits applied for each hour thereafter an 'Incident'	Four Hours Credits double for all hours thereafter.

Severity Level	Description of Deficiency (any one of the following)	Service Response Timeframe	Service Resolution Time
2 Severe	An individual location cannot be monitored or recorded / or sound quality has severely deteriorated /or the ICSS cannot transfer data to storage media / or the Contractor's supplied Workstation or Computer is intermittently malfunctioning / or the ICSS cannot retrieve necessary data for generating reports.	Four Hours Credits applied for each hour thereafter an 'Incident'	Eight Hours Credits double for all hours thereafter.
3 Minor	The ICSS's responses are slower than normal, however proper operations are occurring/or keyboard, mouse or printer is malfunctioning.	Eight Hours Credits applied for each hour thereafter an 'Incident'	24 Hours Credits commence on hour thereafter.
4 Cosmetic	The ICSS's Hardware is damaged but functioning (e.g., key missing from keyboard/key on keyboard sticking)	24 Hours Credits applied for each hour thereafter an 'Incident'	Resolve Incident within three Business Days. Credits commence on Day 4 for each Day thereafter, 8am-5pm. Each Day thereafter an 'Incident'.

4.3.3 Deficiency Resolution Process

For any Deficiency reported by the County or discovered by Contractor, Contractor must immediately commence corrective action. Contractor must correct all Deficiencies within the resolution times specified above. Contractor must also immediately commence to develop a workaround or a fix for any Severity Level 1 or Severity Level 2 Deficiency (hereinafter "Major Deficiency"). The County and Contractor must agree on the Deficiency resolution, whether by a permanent solution or a temporary workaround, as determined by the County.

Contractor must provide the best level of effort to correct all Deficiencies within the prescribed resolution times. In the event Contractor fails to correct a Deficiency within the prescribed resolution time, Contractor must provide the County with a written

or electronic report that includes a detailed explanation of the status of such Deficiency, preliminary actions taken, detailed mitigation plans and an estimated time for completing the correction of such Deficiency. This process will be repeated until the Deficiency is resolved, and the resolution is approved by County Project Manager. The parties will jointly cooperate during this period.

4.3.4 Severity Level Adjustment

The County may escalate or downgrade the Severity Level of a Deficiency if the Deficiency meets the definition of the Severity Level as escalated or downgraded. A Deficiency may also be mutually escalated by the County and Contractor if the Deficiency persists or reoccurs, as determined by County Project Manager. At the time the Deficiency is escalated or downgraded, an appropriate timeline will be applied for resolution of such Deficiency in accordance with Paragraph 4.2.1 (Problem Correction Priorities) of this SLA. Contractor may request an exception to the prescribed timeline when there are extenuating circumstances. Such request may or may not be granted at the sole and absolute discretion of County Project Manager.

If a workaround may be provided by Contractor for a Deficiency, the County and Contractor may agree to downgrade the Severity Level of such Deficiency until an agreed-upon date. If a permanent fix is not provided by such agreed-upon date, the County will have sole discretion to escalate the Severity Level back to the original Severity Level or higher, as provided herein.

4.4 Deficiency Credits

4.4.1 The ICSS is expected to be operational and free of Deficiencies with 100% or 99.5% availability, except for pre-approved ICSS maintenance. Performance will be measured monthly. In the event Contractor fails to meet the availability requirements, Contractor must provide Deficiency Credits to the County as follows:

a. Contractor must credit the County the amount of $300.00 per hour, per individually impacted component, for each Severity Level 1 ICSS Deficiency that is not resolved within the applicable response time set forth in Paragraphs 4.3.1 (Inmate Telephone System – Response Times for Functionalities other than Monitoring) and 4.3.2 (Inmate Telephone System – Response Times for Monitoring Functionalities) of this SLA.

In instances where such a Deficiency exists, Contractor must pay the Deficiency Credits from the time the Deficiency began

until the time the ICSS Deficiency is fully resolved, based on 1-hour increments.

b. Contractor must credit the County an amount of $200.00 per hour, per individually impacted component, for each Severity Level 2 ICSS Deficiency that is not resolved within the applicable response time set forth in Paragraphs 4.3.1 (Inmate Telephone System – Response Times for Functionalities other than Monitoring) and 4.3.2 (Inmate Telephone System – Response Times for Monitoring Functionalities) of this SLA.

   In instances where such a Deficiency exists, Contractor must pay the Deficiency Credits from the time the Deficiency began until the time the ICSS Deficiency is fully resolved, based on full 1-hour increments.

c. Contractor must credit the County an amount of $100.00 per 24-hour period, per individually impacted component, for each Severity Level 3 or 4 ICSS Deficiency that is not resolved response time set forth in Paragraphs 4.3.1 (Inmate Telephone System – Response Times for Functionalities other than Monitoring) and 4.3.2 (Inmate Telephone System – Response Times for Monitoring Functionalities) of this SLA.

In instances where such a Deficiency exists, Contractor must pay the Deficiency Credits based on 24-hour increments from the time the Deficiency began until the time the ICSS Deficiency is fully resolved. Deficiency Credits in this instance will not accrue for any partial 24-hour period.

4.4.2 Deficiency Credits will be assessed as follows:

a. County Project Manager or Contactor are advised by either party of a Severity Level 1, 2, 3, or 4 ICSS Deficiency occurring anywhere within the ICSS.

b. Once it is determined that Deficiency Credits are owed, Contractor begins calculating the Downtime credit, and upon successful resolution of the Deficiency, a dollar amount must be given in writing (via email with a follow up telephone call) to County Project Manager within five Business Days.

c. County Project Manager will verify the amount given by Contractor and approve or deny the Downtime credit amount.

d. Deficiency Credits, in any amount, are not and will not be considered as penalties, and when assessed, will be deducted from the County's payment(s) due to Contractor.

PRICING SCHEDULES

[NOT ATTACHED TO CONTRACT; SEE EXHIBITS 5a (TELEPHONE RATES AND PAYMENT SCHEDULE), 5b (TABLET RATES AND PAYMENT SCHEDULE), AND 5c (DIGITIZED INMATE POSTAL MAIL SERVICES RATES AND PAYMENT SCHEDULE) OF APPENDIX B (REQUIRED FORMS) TO THE RFP]

COUNTY'S ADMINISTRATION

CONTRACT NO. _____

SHERIFF PROJECT DIRECTOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

SHERIFF PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

PROBATION PROJECT DIRECTOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

COUNTY'S ADMINISTRATION

PROBATION PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

COUNTY CONTRACT COMPLIANCE MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

CONTRACTOR'S ADMINISTRATION

CONTRACTOR NAME: _____

CONTRACT NO: _____

CONTRACTOR PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-mail Address: _____

CONTRACTOR SYSTEM ADMINISTRATOR(S):

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-mail Address: _____

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-mail Address: _____

CONTRACTOR'S ADMINISTRATION

CONTRACTOR'S AUTHORIZED OFFICIAL(S):

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

NOTICES TO CONTRACTOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

E-Mail Address: _____

FORMS REQUIRED AT THE TIME OF CONTRACT EXECUTION

F1-IT CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

OR

F2-IT CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

F3-IT CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

Contractor Name: _____ Contract No.: _____

GENERAL INFORMATION:

Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that Contractor employees, consultants, outsourced vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced contract.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agree that they will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any data or information received to County's Project Manager.

Contractor and Contractor's Staff agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation,

CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

Contractor proprietary information and all other original materials produced, created, or provided to Contractor and Contractor's Staff under the above-referenced contract. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during this employment, Contractor and Contractor's Staff must keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

COPYRIGHT ASSIGNMENT AGREEMENT

Contractor and Contractor's Staff agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by Contractor and Contractor's Staff in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom will be the sole property of the County. In this connection, Contractor and Contractor's Staff hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, Contractor and Contractor's Staff agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit H2, attached hereto and incorporated herein by reference.

The County will have the right to register all copyrights in the name of the County of Los Angeles and will have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject them to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

Contractor Name: _____ Contract No.: _____

Employee Name: _____

GENERAL INFORMATION:

Your employer referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Employee Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that Contractor referenced above is my sole employer for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon my employer for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced contract is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation will result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by my employer for the County. I have read this agreement and have taken due time to consider it prior to signing.

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between my employer and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to my immediate supervisor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than my employer or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me during this employment, I must keep such information confidential.

I agree to report to my immediate supervisor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to my immediate supervisor upon completion of this contract or termination of my employment with my employer, whichever occurs first.

COPYRIGHT ASSIGNMENT AGREEMENT

I agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by me in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom will be the sole property of the County. In this connection, I hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, I agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit H1, attached hereto and incorporated herein by reference.

The County will have the right to register all copyrights in the name of the County of Los Angeles and will have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

Contractor Name: _____ Contract No.: _____

Non-Employee Name: _____

GENERAL INFORMATION:

Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Non-Employee Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

NON-EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that Contractor referenced above has exclusive control for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon the Contractor referenced above for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced contract is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation will result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by the above-referenced Contractor for the County. I have read this agreement and have taken due time to consider it prior to signing. I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between the above-referenced Contractor and the

CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to the above-referenced Contractor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information, and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than the above-referenced Contractor or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me, I must keep such information confidential.

I agree to report to the above-referenced Contractor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to the above-referenced Contractor upon completion of this contract or termination of my services hereunder, whichever occurs first.

COPYRIGHT ASSIGNMENT AGREEMENT

I agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by me in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom will be the sole property of the County. In this connection, I hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, I agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit H1, attached hereto and incorporated herein by reference.

The County will have the right to register all copyrights in the name of the County of Los Angeles and will have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____


THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.
Any fire station. Any hospital. Any time.
1.877.222.9723
BabySafeLA.org
No shame | No blame | No names
21
FIRE STATION
98

Some parents of newborns can find themselves in difficult circumstances. Sadly, babies are sometimes harmed or abandoned by parents who feel that they're not ready or able to raise a child. Many of these mothers or fathers are afraid and don't know where to turn for help.

This is why California has a Safely Surrendered Baby Law, which gives parents the choice to legally leave their baby at any hospital or fire station in Los Angeles County.

FIVE THINGS YOU NEED TO KNOW ABOUT BABY SAFE SURRENDER

1. Your newborn can be surrendered at any hospital or fire station in Los Angeles County up to 72 hours after birth.
2. You must leave your newborn with a fire station or hospital employee.
3. You don't have to provide your name.
4. You will only be asked to voluntarily provide a medical history.
5. You have 14 days to change your mind; a matching bracelet (parent) and anklet (baby) are provided to assist you if you change your mind.

No shame | No blame | No names

BabySafeLA.org

ABOUT THE BABY SAFE SURRENDER PROGRAM

In 2002, a task force was created under the guidance of the Children's Planning Council to address newborn abandonment and to develop a strategic plan to prevent this tragedy.

Los Angeles County has worked hard to ensure that the Safely Surrendered Baby Law prevents babies from being abandoned. We're happy to report that this law is doing exactly what it was designed to do: save the lives of innocent babies. Visit BabySafeLA.org to learn more.

No shame | No blame | No names

ANY FIRE STATION.
ANY HOSPITAL.
ANY TIME.

1.877.222.9723
BabySafeLA.org

THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.

BabySafeLA.org

No shame | No blame | No names

FROM SURRENDER TO ADOPTION: ONE BABY'S STORY

Los Angeles County firefighter Ted and his wife Becki were already parents to two boys. But when they got the call asking if they would be willing to care for a premature baby girl who'd been safely surrendered at a local hospital, they didn't hesitate.

Baby Jenna was tiny, but Ted and Becki felt lucky to be able to take her home. "We had always wanted to adopt," Ted says, "but taking home a vulnerable safely surrendered baby was even better. She had no one, but now she had us. And, more importantly, we had her."

Baby Jenna has filled the longing Ted and Becki had for a daughter—and a sister for their boys. Because her birth parent safely surrendered her when she was born, Jenna is a thriving young girl growing up in a stable and loving family.

ANSWERS TO YOUR QUESTIONS

Who is legally allowed to surrender the baby?
Anyone with lawful custody can drop off a newborn within the first 72 hours of birth.

Do you need to call ahead before surrendering a baby?
No. A newborn can be surrendered anytime, 24 hours a day, 7 days a week, as long as the parent or guardian surrenders the child to an employee of the hospital or fire station.

What information needs to be provided?
The surrendering adult will be asked to fill out a medical history form, which is useful in caring for the child. The form can be returned later and includes a stamped return envelope. No names are required.

What happens to the baby?
After a complete medical exam, the baby will be released and placed in a safe and loving home, and the adoption process will begin.

What happens to the parent or surrendering adult?
Nothing. They may leave at any time after surrendering the baby.

How can a parent get a baby back?
Parents who change their minds can begin the process of reclaiming their baby within 14 days by calling the Los Angeles County Department of Children and Family Services at (800) 540-4000.

If you're unsure of what to do:
You can call the hotline 24 hours a day, 7 days a week and anonymously speak with a counselor about your options or have your questions answered.

1.877.222.9723 or BabySafeLA.org
English, Spanish and 140 other languages spoken.

FORMS REQUIRED AT COMPLETION OF THE CONTRACTS INVOLVING INTELLECTUAL PROPERTY DEVELOPED/DESIGNED BY CONTRACTOR. THE INTELLECTUAL PROPERTY DEVELOPED/DESIGNED BECOMES PROPERTY OF THE COUNTY AFTER CREATION OR AT THE END OF THE CONTRACT TERM.

H1 INDIVIDUAL'S ASSIGNMENT AND TRANSFER OF COPYRIGHT

H2 CONTRACTOR'S ASSIGNMENT AND TRANSFER OF COPYRIGHT

H3 NOTARY STATEMENT FOR ASSIGNMENT AND TRANSFER OF COPYRIGHT

INDIVIDUAL'S ASSIGNMENT AND TRANSFER OF COPYRIGHT

For good and valuable consideration, receipt of which is hereby acknowledged, the undersigned, _____, an individual ("Grantor"), does hereby assign, grant, convey and transfer to the County of Los Angeles, California ("Grantee") and its successors and assigns throughout the world in perpetuity, all of Grantor's right, title and interest of every kind and nature in and to all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types (including, without limitation, those items listed on Schedule A, attached hereto and incorporated herein by reference) developed or acquired, in whole or in part, under the Agreement described below, including, but not limited to, all right, title and interest in and to all copyrights and works protectable by copyright and all renewals and extensions thereof (collectively, the "Works"), and in and to all copyrights and right, title and interest of every kind or nature, without limitation, in and to all works based thereon, incorporated in, derived from, incorporating, or related to, the Works or from which the Works are derived.

Without limiting the generality of the foregoing, the aforesaid conveyance and assignment will include, but is not limited to, all prior choses-in-action, at law, in equity and otherwise, the right to recover all damages and other sums, and the right to other relief allowed or awarded at law, in equity, by statute or otherwise.

_____ and Grantee have entered into County of Los Angeles Contract Number

_____, dated _____, as amended by Amendment

Number_____, dated _____,

{NOTE to Preparer: reference all existing Amendments} as the same hereafter may be amended or otherwise modified from time to time (the "Contract").

_____ _____

Grantor's Signature Date

Grantor's Printed Name: _____

Grantor's Printed Position: _____

CONTRACTOR'S ASSIGNMENT AND TRANSFER OF COPYRIGHT

For good and valuable consideration, receipt of which is hereby acknowledged, the undersigned, _____, a _____, ("Grantor") does hereby assign, grant, convey and transfer to the County of Los Angeles, California ("Grantee") and its successors and assigns throughout the world in perpetuity, all of Grantor's right, title and interest of every kind and nature in and to all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training aids, training documentation and aids, and other information and/or tools of all types (including, without limitation, those items listed on Schedule A, attached hereto and incorporated herein by reference) developed or acquired, in whole or in part, under the Agreement described below, including, but not limited to, all right, title and interest in and to all copyrights and works protectable by copyright and all renewals and extensions thereof (collectively, the "Works"), and in and to all copyrights and right, title and interest of every kind or nature, without limitation, in and to all works based thereon, incorporated in, derived from, incorporating or relating to, the Works or from which the Works are derived.

Without limiting the generality of the foregoing, the aforesaid conveyance and assignment will include, but is not limited to, all prior choices-in-action, at law, in equity and otherwise, the right to recover all damages and other sums, and the right to other relief allowed or awarded at law, in equity, by statute or otherwise

Grantor and Grantee have entered into County of Los Angeles Contract Number _____

for _____,

dated _____, as amended by Amendment Number _____, dated _____,

{NOTE to Preparer: reference all existing Amendments} as the same hereafter may be amended or otherwise modified from time to time (the "Contract").

_____ _____

Grantor's Signature Date

Grantor's Printed Name: _____

Grantor's Position: _____

(To Be Completed By County and attached to H1 and/or H2)

REQUIRED ONLY IF COPYRIGHT IS TO BE REGISTERED WITH COPYRIGHT BUREAU

STATE OF CALIFORNIA)
) ss.
COUNTY OF LOS ANGELES)

On _____, 20___, before me, the undersigned, a Notary Public in and for the State of California, personally appeared _____, personally known to me or proved to me on the basis of satisfactory evidence to be the _____ of _____, the corporation that executed the within Assignment and Transfer of Copyright, and further acknowledged to me that such corporation executed the within Assignment and Transfer of Copyright pursuant to its bylaws or a resolution of its Board of Directors.

WITNESS my hand and official seal.

_____
NOTARY PUBLIC

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

The County of Los Angeles ("County") is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit ("Exhibit") sets forth the County and Contractor's commitment and agreement to fulfill each of their obligations under applicable state or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by Contractor before the Effective Date of the Contract and maintained throughout the term of Contract.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Contractor (the "Contract") and any other agreements between the parties. However, it is Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of Contract by Contractor, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. To the extent there are conflicts between this Exhibit and the Contract, this Exhibit will prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this exhibit.

a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

c. **County Information:** all Data and Information belonging to the County.

d. **Data:** a subset of Information comprised of qualitative or quantitative values.

e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.

g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.

i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

j. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** Contractor must maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this Contract.

Contractor's Information Security Program must include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Contractor employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

Contractor must exercise the same degree of care in safeguarding and protecting County Information that Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

Contractor's Information Security Program must:

- Protect the Confidentiality, Integrity, and Availability of County Information in the Contractor's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to Contractor.

b. **Privacy Program.** Contractor must establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. Contractor's Privacy Program must include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Contractor employees, agents, and volunteers. Contractor's Privacy Policies, guidelines, and procedures must be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. Contractor's Privacy Program must perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

Contractor must exercise the same degree of care in safeguarding the privacy of County Information that Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

Contractor's Privacy Program must include:

- A Privacy Program framework that identifies and ensures that Contractor complies with all applicable laws and regulations;
- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;
- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- A training program that covers Privacy Policies, protocols and awareness;
- A response plan to address privacy Incidents and privacy breaches; and
- Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County will retain exclusive rights and ownership thereto. County Information must not be used by Contractor for any purpose other than as required under this Contract, nor will such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Contractor, or commercially exploited or otherwise used by, or on behalf of, Contractor, its officers, directors, employees, or agents. Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. Contractor specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

Contractor may use County Information only as necessary to carry out its obligations under this Contract. Contractor must collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to, (i) any state and federal law governing the protection of personal Information, (ii) any state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. SHARING COUNTY INFORMATION AND DATA

Contractor must not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. CONFIDENTIALITY

a. **Confidentiality of County Information.** Contractor agrees that all County Information is Confidential and proprietary to the County regardless of whether such Information was disclosed intentionally or unintentionally, or marked as "confidential".

b. **Disclosure of County Information.** Contractor may disclose County Information only as necessary to carry out its obligations under this Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of the County's contract administrator in consultation with the County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, Contractor must notify the County's contract administrator immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under the Contract, Contractor may encounter County Non-public Information ("NPI") in the course of performing this Contract, including, but not limited to, licensed technology, drawings,

schematics, manuals, sealed court records, and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. Contractor must not disclose or publish any County NPI and material received or used in performance of this Contract. This obligation is perpetual.

d. **Individual Requests.** Contractor must acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. Contractor must have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County within seven (7) calendar days. If an individual makes a request directly to Contractor involving County Information, Contractor must notify the County within five (5) calendar days and the County will coordinate an appropriate response, which may include instructing Contractor to assist in fulfilling the request. Similarly, if Contractor receives a privacy or security complaint from an individual regarding County Information, Contractor must notify the County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.

e. **Retention of County Information.** Contractor must not retain any County Information for any period longer than necessary for Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. CONTRACTOR EMPLOYEES

Contractor must perform background and security investigation procedures in the manner prescribed in this section unless the Contract prescribes procedures for conducting background and security investigations and those procedures are no less stringent than the procedures described in this section.

To the extent permitted by applicable law, Contractor must screen and conduct background investigations on all Contractor employees and Subcontractors as appropriate to their role, with access to County Information for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include State, local, and federal-level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law, and will be repeated on a regular basis. The fees associated with the background investigation will be at the expense of Contractor, regardless of whether the member of Contractor's staff passes or fails the background investigation. Contractor, in compliance with its legal obligations, must conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

Contractor must require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the Contract, and sign an appropriate written Confidentiality/non-disclosure agreement with Contractor.

Contractor must supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks, and Threats. Contractor agrees that training will cover, but may not be limited to the following topics:

a) **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

b) **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.

c) **Handling of County Information:** The proper identification, storage, transfer, archiving, and destruction of County Information.

d) **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.

e) **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.

f) **Privacy:** Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

Contractor must have an established set of procedures to ensure Contractor's employees promptly report actual and/or suspected breaches of security.

8. SUBCONTRACTORS AND THIRD PARTIES

The County acknowledges that in the course of performing its services, Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Exhibit will also apply to all Subcontractors and third parties. Contractor or third party will be subject to the following terms and conditions: (i) each Subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Exhibit; and (ii) Contractor will be and remain fully liable for the acts and omissions of each Subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under this Contract.

Contractor must obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting services subject to this Exhibit.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information must be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

Contractor will encrypt County Information transmitted on networks outside of Contractor's control with Transport Layer Security (TLS) or Internet Protocol Security **(**IPSec**)**, at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, Contractor must not store County Information in the cloud or in any other online storage provider without written authorization from the County's Chief Information Security Officer. All mobile devices storing County Information must be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by the County's Chief Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

Contractor must return or destroy County Information in the manner prescribed in this section unless the Contract prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this section.

a. **Return or Destruction.** Upon County's written request, or upon expiration or termination of this Contract for any reason, Contractor must (i) promptly return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of this Contract; and (iii) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be returned to the County, Contractor must provide a written attestation on company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, Contractor must provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination or expiration of the Contract or at any time upon the County's request, Contractor must return all hardware, if any, provided by the County to Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. **Method of Destruction.** Contractor must destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging, or destroying electronic media containing County Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" such that the County Information cannot be retrieved. Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County contract manager within ten (10) days of termination or expiration of the Contract or at any time upon the County's request. On termination or expiration of this Contract, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by Contractor hereunder), at the County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry

badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

Contractor must: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

Contractor must have business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-up data; (iii) securely transfer County Information to and from back-up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups must be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. ACCESS CONTROL

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by the County Project Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements will apply to back-up media stored by Contractor at off-site facilities.

Contractor must implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services must be controlled, including, but not limited to, the use of industry standard and properly configured firewalls;

b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging;

c. Contractor will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner;

d. Applications will include access control to limit user access to County Information and application system functions;

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor must record, review and act upon all events in accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, Contractor must ensure all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, Contractor must:

a. Promptly notify the County's Chief Information Security Officer, the Departmental Information Security Officer, and the County's Chief Privacy Officer of any Incidents involving County Information, within twenty-four (24) hours of detection of the Incident. All notifications must be submitted via encrypted email and telephone.

County Chief Information Security Officer and Chief Privacy Officer email
CISO-CPO_Notify@lacounty.gov

Chief Information Security Officer:
Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 253-5659

Chief Privacy Officer:
Lillian Russell
Chief Privacy Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 351-5363

Departmental Information Security Officer:
Fransiscus X. Gunawan (DISO)
Departmental Information Security Officer
12440 Imperial Hwy Suite 400 E
Norwalk, CA 90650
(562) 345-4181
fxgunawa@lasd.org

b. Include the following Information in all notices:

i. The date and time of discovery of the Incident,

ii. The approximate date and time of the Incident,

iii. A description of the type of County Information involved in the reported Incident, and

iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.

v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's written request, without charge, unless the Incident was caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to Contractor, and unless prohibited by law, Contractor must provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.

f. Allow the County or its third-party designee at the County's election to perform audits and tests of Contractor's environment that may include, but are not limited to, interviews of relevant employees, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

Notwithstanding any other provisions in this Contract and Exhibit, Contractor will be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY will constitute a material breach of this Contract and be grounds for immediate termination of this Contract in the exclusive discretion of the County.

16. AUDIT AND INSPECTION

a. **Self-Audits.** Contractor must periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost

and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by the County.

Contractor must have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Contractor must provide the audit results and any corrective action documentation to the County promptly upon its completion at the County's request. With respect to any other report, certification, or audit or test results prepared or received by Contractor that contains any County Information, Contractor must promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in Contractor's Information systems, products, and services, and the corresponding steps taken by Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section must be provided at no additional charge to the County.

b. **County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, will have the right to audit Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon the County's request Contractor must complete a questionnaire regarding Contractor's Information Security and/or program. The County will pay for the County requested audit unless the auditor finds that Contractor has materially breached this Exhibit, in which case Contractor must bear all costs of the audit**;** and if the audit reveals material non-compliance with this Exhibit, the County may exercise its termination rights underneath the Contract.

Such audit will be conducted during Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Contractor's normal business operations. The County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. Contractor must cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access will extend to any regulators with oversight of the County. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

When not prohibited by regulation, Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor or a third party; and (ii) corrective actions or modifications, if any, Contractor will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

Contractor must secure and maintain cyber liability insurance coverage in the manner prescribed in Paragraph 8.25.7 (Cyber Liability Insurance) of the Contract**.**

18. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the Contract, Contractor agrees to indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers,

agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to:

- Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;
- Contractor's failure to perform or comply with any terms and conditions of this Contract or related agreements with the County; and/or,
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on Contractor's systems or networks (including all costs and expenses incurred by the County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Notwithstanding the preceding sentences, the County will have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County will be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

This Exhibit J is available in a fillable form. To request, please contact the County contact listed in Paragraph 6.2 of the RFP.
For your reference, a list of acronyms can be found at the end of this document.

Legend	
M = Mandatory Requirement	**O** = Optional Requirement
D = Requires Development / Programming to meet the requirement Development / Programming is required when the System / Application cannot be configured to meet the business functional and technical requirements. Development requires programming or significant changes to the underlying Database. This can include the development of new modules for the application specific for the requirements and/or programming changes to the base application requiring a separate program tree that needs to be maintained by the vendor for updates.	**C** = Requires Configuration only to meet the requirement Configuration utilizes the table driven or report / screen formatting parameters built into the application itself. The key to configuration is that when the application is upgraded by the vendor the configuration parameters are carried forward with the new release and do not need to be reconfigured.
B = Meets the requirement out of the Box	**X** = Can not meet this requirement
PROPOSERS MUST PROVIDE A RESPONSE FOR ALL REQUIREMENTS. **Failure to response to each requirement will result in point deductions from Proposer's evaluation score.**	

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
	ICSS				
1.0	The ICSS provides:		ICSS		
1.0 a	An automated operator telephone system.	M	ICSS		
1.0 b	Call billing services.	M	ICSS		
1.0 c	Call services throughout the continental 48 states (including the District of Columbia, Alaska and Hawaii).	M	ICSS		
1.0 d	International Call services throughout Canada, Mexico, South America, and to over-seas destinations.	M	ICSS		
1.0 e	A secured web-based ITMS.	M	ICSS		
1.1	The ICSS easily shares data (secure web-services, API's, and export) with other law enforcement agencies/prisons, whether by electronic data stream or by delayed delivery methods. Shared data includes pre-recorded calls, call logs, voice mail messages, or analytical data as authorized by County.	M	ICSS		
1.2	The ICSS monitors inmate telephone operations at Sheriff and Probation Facilities.	M	ICSS		
1.3	The ICSS alerts Contractor System Administrator when system problems or outages occur.	M	ICSS		
1.4	The ICSS provides System adminstration and investigative functions at remote locations and County facilities via dedicated System Administrative Consoles and authorized ITMS web-based access.	M	ICSS		
1.5	The ICSS complies with the ADA and Title 24 of the Board of State and Community Corrections (BSCC.CA.GOV), and is designed for use by the hearing impared.	M	ICSS		
1.6	The ICSS supports California Relay System profile, agreed upon by concerned County Project Director.	M	ICSS		
	ITMS				
2.0	The ITMS allows telephone instruments to be turned on/off remotely.	M	ITMS		
2.1	The ITMS includes an on/off switch (System Administration Kill Switch) in selected locations within each Sheriff and Probation Facility that can function:		ITMS		
2.1 a	Manually.	M	ITMS		
2.1 b	Automatically.	M	ITMS		
2.2	The ITMS provides software-based capability of controlling the Telephone Instruments including, but not limited to:		ITMS		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
2.2 a	Muting the Inmate's ability to speak to the call recipient until the call is accepted.	M	ITMS		
2.2 b	Disabling the telelphone keypad during a call.	M	ITMS		
2.3	The ITMS allows authorized users to turn off/on the following, from any County-authorized computer:		ITMS		
2.3 a	Individual Telephone Instruments.	M	ITMS		
2.3 b	A specified group of Telephone Instruments.	M	ITMS		
2.3 c	All Telephone Instruments.	M	ITMS		
2.4	The ITMS allows authorized user to enable/disable Inmate telephones at Facilities by:		ITMS		
2.4 a	Telephone Instrument.	M	ITMS		
2.4 b	Cellblock.	M	ITMS		
2.4 c	Floor.	M	ITMS		
2.4 d	Day room.	M	ITMS		
2.4 e	Dormitory.	M	ITMS		
2.4 f	Pod.	M	ITMS		
2.4 g	Facility.	M	ITMS		
2.4 h	System-wide.	M	ITMS		
2.4 i	Time of day.	M	ITMS		
2.4 j	Day of the week and/or weekends.	M	ITMS		
2.5	The ITMS allows Users to lock recordings.		ITMS		
2.5 a	Locked recordings cannot be unlocked without the approval of the appropriate authorized User.	M	ITMS		
2.5 b	Locked recordings can only be deleted by the appropriate authorized User.	M	ITMS		
2.6	The ITMS displays historical User data including, but not limited to:		ITMS		
2.6 a	A list of Users who opened the same call recording.	M	ITMS		
2.6 b	Date when User(s) were granted access to the System.	M	ITMS		
2.6 c	Name of individual who authorized access to User(s).	M	ITMS		
2.7	The ITMS displays:		ITMS		
2.7 a	Data on copied files containing each User’s information (e.g., User name, date and time of each copy).	M	ITMS		
2.7 b	Attempted User logon transactions for each logon User name (e.g., the date and time of attempted logon and activity).	M	ITMS		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
2.7 c	Successful User logon transactions for each logon User name (e.g., the date and time of successful logon and activity).	M	ITMS		
2.8	The ITMS provides a feature that allows Users to attach “notes” that provide additional documentation to Call Records.	M	ITMS		
2.9	The ITMS' "notes" feature meets the following criteria:		ITMS		
2.9 a	Logs notes by denoting the User name, and the date and time of entry.	M	ITMS		
2.9 b	Allows notes to be modified.	M	ITMS		
2.9 c	Allows notes to be printed.	M	ITMS		
2.9 d	There is no limit to the amount of characters typed into the notes field.	M	ITMS		
2.9 e	Stores notes via the System as long as the associated call remains accessible.	M	ITMS		
2.10	The ITMS allows calls to be retrieved immediately upon request, without submitting requests for individual audio files to participating agencies.	M	ITMS		
2.11	The ITMS platform software:		ITMS		
2.11 a	Utilizes plain English terminology.	M	ITMS		
2.11 b	Avoids codes or symbols that make navigation difficult.	M	ITMS		
2.11 c	Avoids codes or symbols that require referencing separate screens.	M	ITMS		
2.11 d	Avoids codes or symbols that require referencing distal portions of the software to interpret.	M	ITMS		
2.11 e	Is user-friendly, with displays and prompts that are easily understood, intuitive, and employ readily discernable icons that facilitate a convenient User experience.	M	ITMS		
2.11 f	Includes backing up and archiving critical software and databases on a regular basis.	M	ITMS		
	ITS				
3.0	The automated operator telephone system is capable of:		ITS		
3.0 a	Continuous 24/7 operation.	M	ITS		
3.0 b	Establishing connection within 45-seconds of call placement without the need for an Inmate's access to a Live Agent Operator.	M	ITS		
3.0 c	Prompting an Inmate caller to select the desired language by pressing the designated keypad digit.	M	ITS		
3.0 d	Supporting English, Spanish, and other languages as required by the County.	M	ITS		
3.1	The automated operator telephone system identifies the Inmate by validating the Inmate’s Booking number prior to Inmate placing a telephone call.	M	ITS		
3.2	The automated operator telephone system prompts caller to enter the Inmate Booking number by pressing the digits on the Telephone Instrument keypad, followed by Inmate voice verification, and entry of the destination telephone number.	M	ITS		.

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
	INMATE TELEPHONE INSTRUMENTS				
4.0	The ICSS Inmate Telephone Instruments are:		Telephone Instruments		
4.0 a	Line powered (via internal Category three wiring and derived from the platform) with the exception of TDD.	M	Telephone Instruments		
4.0 b	Free from requiring additional power sources or batteries, unless specifically requested by the concerned County Project Manager.	M	Telephone Instruments		
4.0 c	In full compliance with FCC regulations.	M	Telephone Instruments		
4.0 d	In full compliance with UL Standards.	M	Telephone Instruments		
4.0 e	Capable of being installed in compliance with NEC standards.	M	Telephone Instruments		
4.0 f	New.	M	Telephone Instruments		
4.0 g	In working order.	M	Telephone Instruments		
4.0 h	Free of defects.	M	Telephone Instruments		
4.0 i	Of rugged construction.	M	Telephone Instruments		
4.0 j	Tamperproof.	M	Telephone Instruments		
4.0 k	Encased in rugged steel housings.	M	Telephone Instruments		
4.0 l	Equipped with shockproof keypads.	M	Telephone Instruments		
4.0 m	Water resistant.	M	Telephone Instruments		
4.0 n	Fire resistant.	M	Telephone Instruments		
4.0 o	Equipped with key-locked mountings to the wall.	M	Telephone Instruments		
4.0 p	Configured with a braided steel receiver cord exactly 12-inches in length to reduce the risk of suicide by hanging.	M	Telephone Instruments		
4.0 q	Made of stainless steel or in combination with a corrosion resistant finish.	M	Telephone Instruments		
4.0 r	Capable of being mounted to poured concrete walls, block walls, stainless steel shrouded columns, and/or protected external enclosures.	M	Telephone Instruments		
4.0 s	Suitable for indoor installation.	M	Telephone Instruments		
4.0 t	Suitable for outdoor installation.	M	Telephone Instruments		
4.0 u	Programmed for outgoing call usage only.	M	Telephone Instruments		
4.0 v	Equipped with a heavy chrome metal 12-button keypad.	M	Telephone Instruments		
4.0 w	Suitable for high-use/abuse custody and detention environments.	M	Telephone Instruments		
4.1	The ICSS Inmate Telephone Instruments are not capable of accepting the following as payment:		Telephone Instruments		
4.1 a	Cash.	M	Telephone Instruments		
4.1 b	Credit cards.	M	Telephone Instruments		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
4.1 c	Coins.* *Coin slots (or coin return slots) are welded shut, replaced, covered with metal plates, or otherwise removed.	M	Telephone Instruments		
4.2	The ICSS Inmate Telephone Instruments include mid-size phones measuring approximately 15"H x 8"W x 4"D.* *Cordless Telephone Instruments may be of slightly larger or smaller size, depending on the manufacturer's specifications and availability.	M	Telephone Instruments		
4.3	The ICSS handsets, earpieces, and mouthpieces are of heavy-duty construction with no removable parts.	M	Telephone Instruments		
4.4	The ICSS' Inmate Telephone Instruments include a cradle for a:		Telephone Instruments		
4.4 a	Handset with an armored cord exactly 12-inches in length.	M	Telephone Instruments		
4.4 b	Cordless handset.	M	Telephone Instruments		
	PORTABLE TELEPHONE INSTRUMENTS				
5.0	The ICSS' Portable Telephone Instruments are:		Telephone Instruments		
5.0 a	Provided on wheeled platforms, mounted on a rugged metal cart equipped with at least four rubberized, outer-laced wheel castors, designed to fit through a thirty-six-inch-wide entrance.	M	Telephone Instruments		
5.0 a-i	Cart with marine cord is capable of plugging into a pre-positioned telephone jack.	M	Telephone Instruments		
5.0 b	21"H x 8"W x 6"D at maximum and 10"H x 7"W x 3"D at minimum.	M	Telephone Instruments		
5.0 c	Suitable for indoor installations.	M	Telephone Instruments		
5.0 d	Equipped with a durable metal 12-button keypad.	M	Telephone Instruments		
5.0 e	Corrosion resistant.	M	Telephone Instruments		
5.1	Portable Telephone Instruments include:		Telephone Instruments		
5.1 a	A cradle with a braided armored flex tubing cord.	M	Telephone Instruments		
5.1 b	A handset with a braided armored flex tubing cord.	M	Telephone Instruments		
5.1 c	A marine cord permanently attached to the cart (marine cord will be determined by the concerned County Project Manager).	M	Telephone Instruments		
5.1 d	A true cordless handset telephone availble to be installed at select Facility locations.	M	Telephone Instruments		
5.1 e	An on/off hook switch.	M	Telephone Instruments		
5.1 f	A cordless Vandal Resistant and Armored Speakerphone.	M	Telephone Instruments		
5.2	The ICSS' Portable Telephone Instruments posses the same:		Telephone Instruments		
5.2 a	Monitoring and archiving capabilities as all phones at other Facilities.	M	Telephone Instruments		
5.2 b	Recording capabilities as all phones at other Sheriff's Facilities.	M	Telephone Instruments		
	TDD				
6.0	The ICSS' TDD's meet the following criteria:		Telephone Instruments		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
6.0 a	Comply with ADA regulations and standards.	M	Telephone Instruments		
6.0 b	Operate via the California Relay System Services.	M	Telephone Instruments		
6.0 c	Are capable of recording the text/conversation as with all other audio of Inmate phone calls on the ICSS.	M	Telephone Instruments		
6.0 d	Are equipped with amplified handsets.	M	Telephone Instruments		
6.1	The ITS' TDD Amplified Handsets include a volume control interface.	M	Telephone Instruments		
6.2	The TDD's volume control interface allows inmates to:		Telephone Instruments		
6.2 a	Increase the audio volume of the headset earpiece.	M	Telephone Instruments		
6.2 b	Decrease the audio volume of the headset earpiece.	M	Telephone Instruments		
	PRE-RECORDED BRANDING PROMPTS				
7.0	The ITS' Pre-Recorded Call Branding Prompts feature is as follows:		Call Branding Prompts		
7.0 a	When an inmate places a call, the ITS is capable of playing pre-recorded call branding prompts as specified in Attachment 6 (Pre-recorded Call Branding Prompts) of Exhibit B (Statement of Work Attachments) to the Contract.	M	Call Branding Prompts		
7.0 b	The ICSS provides short, periodic announcements during live calls which do not require Inmate or Customer acknowledgement (e.g., "Call is being recorded" or "Person on the other end of line is an Inmate in a Probation Facility").	M	Call Branding Prompts		
	CALL ACCEPTANCE				
8.0	The ITS requires call recipient to accept a call after the Customer hears the pre-recorded call branding prompts.	M	Call Acceptance		
8.1	Upon acceptance by the call recipient, the ITS unmutes the Inmate's handset and the call proceeds, however, the Inmate's telephone keypad remains disabled throughout the duration of the call.	M	Call Acceptance		
	CALL TERMINATION				
9.0	Upon call termination, the ITS:		Call Termination		
9.0 a	Disconnects the line to the destination telephone number.	M	Call Termination		
9.0 b	Mutes the Inmate's telephone handset.	M	Call Termination		
9.0 c	Disables the telephone keypad, except when responding to prompts initiated by the automated operator.	M	Call Termination		
	CALL DURATION				
10.0	The ITS provides control features for Users to set-up call duration.	M	Call Duration		
10.1	The ITS' call duration feature has the following capabilities:		Call Duration		
10.1 a	Limits each standard Inmate call to a maximum of 60 minutes in length, per call.	M	Call Duration		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
10.1 b	The automated operator ITS has the capability of limiting the duration of Inmate telephone calls, remotely from the System Administrative Consoles (provided under the Contract) by:		Call Duration		
10.1 b-i	Telephone Instrument.	M	Call Duration		
10.1 b-ii	Cellblock.	M	Call Duration		
10.1 b-iii	Floor.	M	Call Duration		
10.1 b-iv	Day room.	M	Call Duration		
10.1 b-v	Dormitory.	M	Call Duration		
10.1 b-vi	Pod.	M	Call Duration		
10.1 b-vii	Facility.	M	Call Duration		
10.1 b-viii	System-wide.	M	Call Duration		
10.1 c	Allows the length of Inmate Calls to be modified at the County's request.	M	Call Duration		
	UNAUTHORIZED CALL INTERRUPTION				
11.0	When unauthorized or illegal activities are detected by either the ITS or an ITMS user, the ITS' Unauthorized Call Interruption feature:		Unathorized Calls		
11.0 a	Interrupts Inmate telephone calls.	M	Unathorized Calls		
11.0 b	Disconnects Inmate telephone calls.	M	Unathorized Calls		
11.0 c	Provides a pre-recorded announcement pertaining to the reason for the call interruption, at the County's discretion.	M	Unathorized Calls		
11.1	On connected Inmate calls in which an Inmate attemps to access special calling features, or presses/dials additional keypad buttons, the ITS is prompted to:		Unathorized Calls		
11.1 a	Detect the call.	M	Unathorized Calls		
11.1 b	Interrupt the call.	M	Unathorized Calls		
11.1 c	Terminate the call.	M	Unathorized Calls		
11.1 d	Flag the call.	M	Unathorized Calls		
	AUTHORIZED CALL LISTS				
12.0	The ITS creates and administers Authorized Call Lists containing the complete list of telephone numbers that specified inmates are permitted to call.	M	Authorized Calls		
12.1	ITMS provides the capability to check the System's list of unauthorized telephone numbers to verify that the Inmate's proposed Authorized Call List does not contain or permit calls to unauthorized telephone numbers.	M	Authorized Calls		
12.1 a	The ITMS rejects any identified unauthorized telephone numbers from the Inmate's Authorized Call List.	M	Authorized Calls		
12.2	The ITS must provide for calls to an Inmate's private attorney or Public Defender to be confidential.	M	Authorized Calls		
12.2 a	The ITS does not monitor or record calls to the Inmate's private attorney or Public Defender.	M	Authorized Calls		

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
12.2 b	The ITS compares dialed numbers with a list of telephone numbers known to be for private attorneys and/or public defenders before completing a connection.* *This list is compiled from the State Bar of California database, and is capable of being updated or modified frequently. If a number appears on this list, the ITS automatically disables monitoring and recording of that call.	M	Authorized Calls		
	CALL BLOCKING REQUIREMENTS				
13.0	The ITS' Call Blocking feature has the following functionalities:		Call Blocking Requirements		
13.0 a	Maintains a database containing blocked telephone numbers.	M	Call Blocking Requirements		
13.0 b	Detects and blocks calls electronically and independently, via designated System Administrative Consoles, by:		Call Blocking Requirements		
13.0 b-i	Area code.	M	Call Blocking Requirements		
13.0 b-ii	Prefix.	M	Call Blocking Requirements		
13.0 b-iii	Destination numbers.	M	Call Blocking Requirements		
13.0 b-iv	Local operator calls (0).	M	Call Blocking Requirements		
13.0 b-v	Information (411).	M	Call Blocking Requirements		
13.0 b-vi	Emergency Services (911).	M	Call Blocking Requirements		
13.0 b-vii	Time (555-1212).	M	Call Blocking Requirements		
13.0 b-viii	Business or special service numbers (such as 1-700, 1-800, 1-887, 1-888, 1-900 and 1-976 numbers).	M	Call Blocking Requirements		
13.0 b-ix	Numeric sequences associated with other call carriers for operator services (such as 1-950 numbers).	M	Call Blocking Requirements		
13.0 b-x	Commercially available debit calling cards.	M	Call Blocking Requirements		
13.0 b-xi	Calls likely intended to cause a public nuisance.	M	Call Blocking Requirements		
13.0 b-xii	Long Distance telephone call attempts to by-pass the County's Inmate telephone services, utilizing numeric access codes, such as 1-0-XXX, 1-0-1-0-XXX to alternative calling plans provided by other Long-Distance service providers.	M	Call Blocking Requirements		
13.0 c	Includes System sensitivity modifications and configurations to prevent attempts at Unauthorized Calls, while simultaneously permitting Authorized Calls and avoiding erroneous disconnects.	M	Call Blocking Requirements		
13.0 d	Provides the call recipients with a convenient method for blocking calls from Inmates.* *Proposer must describe, in the comments sections, what method their proposed ICSS provides.	M	Call Blocking Requirements		
13.0 e	Detects and blocks Inmate's call attempts to unauthorized telephone numbers.* *Unauthorized numbers include, but are not limited to, public officials, government agencies, businesses, numbers blocked by family members, etc.	M	Call Blocking Requirements		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
13.1	The ITS reports Inmate's call attempts to unauthorized telephone numbers.	M	Call Blocking Requirements		
13.2	The ITS' Incoming Call Blocking feature has the following capabilities:		Call Blocking Requirements		
13.2 a	Prevents all incoming calls to Inmate telephones in Facilities.	M	Call Blocking Requirements		
13.2 b	Rejects any attempted incoming calls.	M	Call Blocking Requirements		
13.2 c	Records appropriate information (if available) of any attempted incoming calls.	M	Call Blocking Requirements		
13.2 d	Archives any attempted incoming calls.	M	Call Blocking Requirements		
13.2 e	Reports any attempted incoming calls to the County Project Manager via email.	M	Call Blocking Requirements		
13.3	The ITS' Three-way Call Blocking feature has the following capabilities:		Call Blocking Requirements		
13.3 a	Detects attempted three-way calls.	M	Call Blocking Requirements		
13.3 b	Flags attempted three-way calls.	M	Call Blocking Requirements		
13.3 c	Blocks attempted three-way calls.	M	Call Blocking Requirements		
13.3 d	Detects attempted forwarding of Inmate calls.	M	Call Blocking Requirements		
13.3 e	Blocks attempted forwarding of Inmate calls.	M	Call Blocking Requirements		
13.3 f	Disconnects all three-way calls within a default time set in seconds.	M	Call Blocking Requirements		
13.3 g	Sends email notices of detected three way call attempt to County personnel.	M	Call Blocking Requirements		
13.3 h	Records information regarding any detected Inmate three-way call attempt.	M	Call Blocking Requirements		
1.3 i	Records appropriate information regarding all Inmate call forwarding attempts.	M	Call Blocking Requirements		
13.3 j	Archives information regarding any detected Inmate three-way call attempt.	M	Call Blocking Requirements		
13.3 k	Archives appropriate information regarding all Inmate call forwarding attempts.	M	Call Blocking Requirements		
13.3 l	Alerts concerned County Project Manager appropriate information regarding all Inmate call forwarding attempts.	M	Call Blocking Requirements		
13.3 m	Detects any call to an electronic forwarding service phone number such as “Google Voice” or other Internet-based phone call forwarding service.	M	Call Blocking Requirements		
13.3 n	Blocks any call to an electronic forwarding service phone number such as “Google Voice” or other Internet-based phone call forwarding service.	M	Call Blocking Requirements		
13.3 o	Prohibits Inmate telephone calls via a Live Agent Operator (i.e., Inmates limited to placing automated operator assisted calls only).	M	Call Blocking Requirements		
13.3 p	Reports any attempted three-way calls to the County Project Manager via email.	M	Call Blocking Requirements		
	CALL ARCHIVING AND RETRIEVAL				
14.0	The ICSS' Call Archiving and Retrieval feature has the following capabilities:		Call Archiving and Retrieval		
14.0 a	Records all completed and call attempts made from any and all Telephone Instruments within all Facilities.	M	Call Archiving and Retrieval		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
14.0 b	Does not record calls initiated by Pro-Per Inmate booking numbers.	M	Call Archiving and Retrieval		
14.0 c	Captures and records unauthorized activities.	M	Call Archiving and Retrieval		
14.0 d	Archives and immediately allows Users to retrieve all recorded Inmate telephone calls:		Call Archiving and Retrieval		
14.0 d-i	Via any System Administrative Console.	M	Call Archiving and Retrieval		
14.0 d-ii	Via web-based access and/or any SDN computer with Internet capability.	M	Call Archiving and Retrieval		
14.0 e	Records calls to an off-line media for archiving or review.	M	Call Archiving and Retrieval		
14.0 f	All recorded telephone calls (files) include the following data:		Call Archiving and Retrieval		
14.0 f-i	Salutatory call branding information.	M	Call Archiving and Retrieval		
14.0 f-ii	Date the telephone call was placed.	M	Call Archiving and Retrieval		
14.0 f-iii	Time the telephone call was placed.	M	Call Archiving and Retrieval		
14.0 f-iv	Location from which the telephone call was placed.	M	Call Archiving and Retrieval		
14.0 f-v	Telephone number that was dialed.	M	Call Archiving and Retrieval		
14.0 f-vi	Duration of the telephone call.	M	Call Archiving and Retrieval		
14.0 f-vii	Time that the telephone call was terminated.	M	Call Archiving and Retrieval		
14.0 f-viii	Reason that the telephone call was terminated.	M	Call Archiving and Retrieval		
14.0 f-ix	Inmate's Booking number.	M	Call Archiving and Retrieval		
14.0 f-x	Inmate’s voice biometric identification tag.	M	Call Archiving and Retrieval		
14.0 g	Encrypts all County information, within possession, where the information is stored (data at rest requires AES, or equivalent protocol, with cipher strength of 256-bit, or equivalent).	M	Call Archiving and Retrieval		
14.0 h	The recorded call file format is compatible with Microsoft® Windows, Windows 7, Windows 8, and Windows 10 based personal computers, or other format to be determined by County.	M	Call Archiving and Retrieval		
14.0 h-i	Also provides an Apple® MacOS client for Users who wish to access the System on Apple/Macintosh equipment.	M	Call Archiving and Retrieval		
14.0 i	The ITS automatically generates a file name.	M	Call Archiving and Retrieval		
14.0 j	Each call recording file is a unique but systematic naming convention.	M	Call Archiving and Retrieval		
14.0 k	Each recorded telephone call or any copies are security encoded in order to detect any attempted alterations to the recorded telephone call.	M	Call Archiving and Retrieval		
14.0 l	Each call recording file is labeled with a SHA1 hash value by which to validate the call file’s unaltered integrity.	M	Call Archiving and Retrieval		
14.0 m	Provides an audio player in each exported audio call file(s) for ease of use.	M	Call Archiving and Retrieval		

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
14.0 n	The ITS is able to flag or "lock" each individual recording, so that it is retained for investigative purposes indefinitely (beyond the standard specification for all other calls).	M	Call Archiving and Retrieval		
	INMATE VOICEMAIL				
15.0	The ICSS includes an Inmate Voicemail feature which:		Inmate Voicemail		
15.0 a	Allows Inmates and their families a method for communicating without having to successfully complete a person-to-person phone call.	M	Inmate Voicemail		
15.0 b	Allows/Restricts Inmates from leaving outgoing messages.* *This feature is initially turned OFF until instructed otherwise by the County.	M	Inmate Voicemail		
15.0 c	Allows family members outside of Facilities to call a specified phone number, enter the Inmate's booking number, verify the Inmate's name, and record a message not exceeding one minute in duration.	M	Inmate Voicemail		
15.0 d	Inmate's use of the feature does not incur fees.	M	Inmate Voicemail		
15.0 e	Records voicemail messages.	M	Inmate Voicemail		
15.0 f	Logs voicemail messages for a defined period of time.	M	Inmate Voicemail		
15.0 g	Stores voicemail messages for a defined period of time.	M	Inmate Voicemail		
15.0 h	Allows Users to easily retrieve and monitor voicemail messages.	M	Inmate Voicemail		
15.0 i	Allows Users to review messages before delivery to the Inmate.	M	Inmate Voicemail		
15.0 j	Provides a security method for verifying authenticity of recordings.	M	Inmate Voicemail		
15.0 k	Retains voicemails for a period of five years.	M	Inmate Voicemail		
15.1	The ITMS is able to flag (or "lock") certain voicemail messages for investigative purposes and prevent messages so identified from being deleted after five years.	M	Inmate Voicemail		
	ADMINISTRATIVE AND INVESTIGATIVE FUNCTIONS				
16.0	The ITMS' administrative and investigative feature:		Administrative/ Investigative		
16.0 a	Provides the capacity to monitor Inmate telephone calls at all Facilities.	M	Administrative/ Investigative		
16.0 b	Provides a secured web-based program to allow investigators the ability to log into the ITMS from web enabled computers using a two-factor authentication for user login.	M	Administrative/ Investigative		
16.1	The ITMS' administrative and investigative feature includes the following functionalities:		Administrative/ Investigative		
16.1 a	Stores all analytical data.	M	Administrative/ Investigative		
16.1 b	Accesses analytical data available by Ad Hoc and custom filtering.	M	Administrative/ Investigative		
16.1 c	Accesses analytical data by Web service.	M	Administrative/ Investigative		
16.1 d	Performs voice transcription.	M	Administrative/ Investigative		
16.1 e	Performs voice keyword search.	M	Administrative/ Investigative		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
16.1 f	Performs voice keyword blocking.	M	Administrative/ Investigative		
16.1 g	Distinguishes call destination as landline or cellphone.	M	Administrative/ Investigative		
16.1 h	Produces graphs and charts displaying System usage, financial data, call methods, Completed Calls, and calls, whether completed or non-completed, known to be or suspected of being fraudulent.	M	Administrative/ Investigative		
16.1 i	Alerts investigators on a specified confidential phone number to alert the investigators to live calls taking place that have been flagged.	M	Administrative/ Investigative		
16.1 j	Allows investigators to listen to live calls to which they have been alerted.	M	Administrative/ Investigative		
16.1 k	Allows case notes and case note management.		Administrative/ Investigative		
16.1 k-i	Users of the System are able to enter comprehensive notes (no limit on characters) about each individual call.	M	Administrative/ Investigative		
16.1 k-ii	These notes are stored for the life of the Contract and are easily exportable to other documents (Word, Excel, and PDF).	M	Administrative/ Investigative		
16.2	The ITMS provides comprehensive report generation with spider style charting, allowing investigators the ability to see (and drill down) call information (e.g., booking number or specified phone numbers).	M	Administrative/ Investigative		
16.3	The ITMS provides the ability for investigators to flag certain calls and/or booking numbers into specified categories (such as gangs, abusers of the System, or any other specified category as determined by Users of the System).	M	Administrative/ Investigative		
16.4	The ITMS is capable of providing selected recorded files in a self-contained format with high compatibility and user-friendly playback for various configurations of Windows PCs during in court testimony and for investigative purposes.	M	Administrative/ Investigative		
16.5	The ITMS automates and saves speech-to-text recognition allowing investigators to easily search for key words.	M	Administrative/ Investigative		
16.6	The ITMS detects calls that suggest threats to the safety and security of the facility, staff, volunteers, and inmates entrusted to the care of the customer.	M	Administrative/ Investigative		
16.7	The ITMS immediately notifies an investigator and/or investigator group when User-defined phone numbers are associated with:		Administrative/ Investigative		
16.7 a	An individual on a monitor list is dialed by a listed Inmate.	M	Administrative/ Investigative		
16.7 b	A select group on a monitor list is dialed by a listed Inmate and a connection is made to a listed number.	M	Administrative/ Investigative		
16.8	The ITMS allows staff to set up alerts based on keywords and phrases.	M	Administrative/ Investigative		
16.9	The ITMS identifies multiple calls using keywords, identifies specific phone calls from Inmates, and sends an alert to investigative personnel.	M	Administrative/ Investigative		
16.10	The ITMS provides language translation into English, for multi-lingual recorded messages and keyword searches.	M	Administrative/ Investigative		
16.11	The ITMS is able to learn and store new keywords that are not part of the “known” key word.	M	Administrative/ Investigative		
16.12	The ITMS provides a method for an investigator to conference with another investigator to listen in only on a live call being monitored.	M	Administrative/ Investigative		
16.13	The ITMS provides transcripts of calls in near real time.	M	Administrative/ Investigative		
16.14	The ITMS provides a feature to identify phone billing name and address.	M	Administrative/ Investigative		
16.15	The ITMS provides a substantial variety of search and sort features, both investigative and administrative, including:		Administrative/ Investigative		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
16.15 a	Played calls.	M	Administrative/ Investigative		
16.15 b	Recorded calls.	M	Administrative/ Investigative		
16.15 c	Completed calls.	M	Administrative/ Investigative		
16.15 d	Incomplete calls.	M	Administrative/ Investigative		
16.15 e	Copied or downloaded calls.	M	Administrative/ Investigative		
16.15 f	Calls with notes.	M	Administrative/ Investigative		
16.15 g	Note content.	M	Administrative/ Investigative		
16.15 h	Locked calls.	M	Administrative/ Investigative		
16.15 i	Call duration.	M	Administrative/ Investigative		
16.15 j	Manner in which call was initiated.	M	Administrative/ Investigative		
16.15 k	Manner in which call was terminated.	M	Administrative/ Investigative		
16.15 l	Type of call.	M	Administrative/ Investigative		
16.15 m	Calls by key words.	M	Administrative/ Investigative		
16.15 n	Calls by phrases.	M	Administrative/ Investigative		
16.15 o	Calls by tones.	M	Administrative/ Investigative		
16.16	The ITMS provides a method for investigators to utilize “bookmarks” or “timeline markers” to tag a particular location (in time) within a recording for future reference and enter comments or notes within the bookmark. Bookmarks are not retained unless a voice recording file has been downloaded or saved.	M	Administrative/ Investigative		
16.17	The ITMS allows authorized Users to:		Administrative/ Investigative		
16.17 a	Listen to calls in real time for each Telephone Instrument located within a particular Facility.	M	Administrative/ Investigative		
16.17 b	Monitor calls through any County-authorized computer.	M	Administrative/ Investigative		
16.17 c	Monitor calls by sending calls to a designated telephone number (e.g. cell phone, home phone, or office phone without an extension).	M	Administrative/ Investigative		
16.18	Disconnect an Inmate call as it is being monitored, immediately and without warning to parties involved in conversation.	M	Administrative/ Investigative		
16.19	The ITMS protects completed Inmate calls stored for retrieval from fraud and tampering throughout the storage term.	M	Administrative/ Investigative		
16.20	The ITMS provides a means for “dead space” in recorded Inmate telephone calls where no voice is detected, to be eliminated, leaving only the actual voice recordings in a compressed/abbreviated format. Such feature does not alter the System capabilities to retain the original file with security envelope.	M	Administrative/ Investigative		
	VOICE BIOMETRICS				
17.0	The ITMS' voice biometric feature includes the following capabilities:		Voice Biometrics		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
17.0 a	Control features for Users to identify voice biometrics.	M	Voice Biometrics		
17.0 b	Interfacing and/or integrating with County's biometrics solution (voice biometrics feature).	M	Voice Biometrics		
17.0 c	Utilizes an initial voice enrollment procedure, Inmates and users of the system are able to complete enrollment from each Telephone Instrument at every Facility.	M	Voice Biometrics		
17.0 d	Does not limit enrollmment to certain phones (such as solely within the Department's Inmate Reception Center); loud environments when enrolling initial voice biometrics are considered and do not limit the Inmate from proceeding.	M	Voice Biometrics		
17.0 e	Identifies the Inmate by validating the Inmate's voice, in response to the pre-recorded System prompt prior to Inmate placing a telephone call.	O	Voice Biometrics		
17.0 f	Matches the Inmate's voice to the recorded sample and either allows or disallows the call to be completed based upon a voice match or non-match.	M	Voice Biometrics		
17.0 g	Flags and terminates failed voice verification attempts via the ITS.	M	Voice Biometrics		
17.0 h	Locks the account after three failed voice verification attempts.	M	Voice Biometrics		
17.0 i	Automatically unlocks the account once an hour has elapsed from failed attempts and allows the Inmate to make additional attempts.	M	Voice Biometrics		
17.0 j	Allows the County to disable the voice biometrics feature at any time.	M	Voice Biometrics		
	SYSTEM ADMINISTRATIVE CONSOLES				
18.0	Equipment and features of Administrative Consoles include, but are not limited to:		Administrative Consoles		
18.0 a	Computer(s).	M	Administrative Consoles		
18.0 b	Monitor(s), minimum of 24 inches.	M	Administrative Consoles		
18.0 c	High-quality color printer(s).	M	Administrative Consoles		
18.0 d	All software necessary to review and monitor phone calls.	M	Administrative Consoles		
18.0 e	All related hardware.	M	Administrative Consoles		
18.0 f	Sufficient processing speed.	M	Administrative Consoles		
18.0 g	Sufficient storage capacity.	M	Administrative Consoles		
18.0 h	Other feature functionality to ensure rapid and efficient retrieval data.	M	Administrative Consoles		
18.0 i	Any ancillary equipment deemed necessary for the monitoring, recording, archiving or retrieval of Inmate calls.	M	Administrative Consoles		
18.1	The ICSS allows the concerned County Project Manager to easily see the status (online, offline, etc.) of each portion/component of the System at any given time.	M	Administrative Consoles		
18.2	The ICSS' System Administrative Consoles provide real-time System status displays, including current operational status of both on-site and remote facilities.	M	Administrative Consoles		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
	SYSTEM SECURITY				
19.0	The ICSS' System Security features include:		System Security		
19.0 a	A secure logon procedure that guards against fraudulent use.	M	System Security		
19.0 b	A feature causing established passwords to auto-expire within a time frame determined by County.	M	System Security		
19.0 c	Security safeguards to control access to the System.	M	System Security		
19.0 d	Levels of permissions that allow County Project Directors the ability to:		System Security		
19.0 d-i	Create User accounts and assign permissions.	M	System Security		
19.0 d-ii	Edit User accounts and assign permissions.	M	System Security		
19.0 d-iii	View User accounts and assign permissions.	M	System Security		
19.0 e	User authentication for County employees must be integrated with Active Directory.		System Security		
19.0 e-i	Detailed definitions for System Administrator, User, or other definable levels of access.	M	System Security		
19.0 f	Capability of displaying:		System Security		
19.0 f-i	Historical User data including, but not limited to, when User(s) were granted access to the System.	M	System Security		
19.0 f-ii	Historical User data including, but not limited to, who authorized access to User(s).	M	System Security		
19.0 f-iii	Data on copied files containing each User's information including, but not limited to, User name, date and time of each copy.	M	System Security		
19.0 f-iv	Attempted User logon transactions for each logon User name, including but not limited to, the date and time of attempted logon and activity.	M	System Security		
19.0 f-v	Successful User logon transactions for each logon User name, including but not limited to, the date and time of successful logon and activity.	M	System Security		
19.0 g	A means by which authorized Users can add numbers to a destination number list associated with an inmate booking number.*	M	System Security		
19.1	Access to the ICSS is Password protected.	M	System Security		
19.2	ITMS Passwords are:		System Security		
19.2 a	Complex.	M	System Security		
19.2 b	Enforced by Active Directory.	M	System Security		
19.2 c	Changed every 90 Days or with more frequency.	M	System Security		
19.2 d	Includes method of deleting/disabling inactive ITMS accounts automatically after specific time period (defined by the County).	M	System Security		
19.3	The ITMS allows the County to restrict or limit ITMS web-based access by IP address.	M	System Security		
	REPORTING REQUIREMENTS				
20.0	The System provides a report that includes detailed call information from recorded calls.	M	Reporting Requirements		
20.1	The System allows authorized users to access and print call recordings for administrative and/or investigative functions including, but not limited to:		Reporting Requirements		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
20.1 a	Deriving total call minutes/duration.	M	Reporting Requirements		
20.1 b	Originating Facility.	M	Reporting Requirements		
20.1 c	Start and end date/time of call.	M	Reporting Requirements		
20.1 d	Phone location.	M	Reporting Requirements		
20.1 e	Destination number.	M	Reporting Requirements		
20.1 f	Manner in which the call started and ended.	M	Reporting Requirements		
20.2	The System provides a report which includes, but is not limited to, the following:		Reporting Requirements		
20.2 a	A unique file name for each recorded call.	M	Reporting Requirements		
20.2 b	A summary information on all:		Reporting Requirements		
20.2 b-i	Attempted calls.	M	Reporting Requirements		
20.2 b-ii	Accepted calls.	M	Reporting Requirements		
20.2 b-iii	Incomplete calls.	M	Reporting Requirements		
20.2 b-iv	Connected calls.	M	Reporting Requirements		
20.2 b-v	Denied calls.	M	Reporting Requirements		
20.3	The System provides a report that tracks the total number of calls by both origination number (Telephone Instrument) and call destination number (number dialed by the Inmates).	M	Reporting Requirements		
20.4	This report includes, but is not limited to:		Reporting Requirements		
20.4 a	The origination number.	M	Reporting Requirements		
20.4 b	Location of the Telephone Instrument within the Facility.	M	Reporting Requirements		
20.4 c	Number of call attempts from the Telephone Instrument.	M	Reporting Requirements		
20.4 d	Number of accepts (calls accepted by the called party from this Telephone Instrument).	M	Reporting Requirements		
20.4 e	Destination number (number dialed by the Inmate).	M	Reporting Requirements		
20.4 f	Number of attempts to the destination number.	M	Reporting Requirements		
20.4 g	Number of calls accepted at the destination number.	M	Reporting Requirements		
20.5	The System provides a report indicating activities associated with destination numbers placed on an alert list provided by County. Calls to specified destination numbers are monitored each time they are dialed by an Inmate.	M	Reporting Requirements		
20.6	This report contains call detail information including, but not be limited to:		Reporting Requirements		
20.6 a	Whether call was recorded.	M	Reporting Requirements		

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
20.6 b	Whether the call had notes attached.	M	Reporting Requirements		
20.6 c	Whether the call was locked.	M	Reporting Requirements		
20.6 d	Facility name.	M	Reporting Requirements		
20.6 e	Destination number.	M	Reporting Requirements		
20.6 f	Date/time of alert.	M	Reporting Requirements		
20.6 g	Call length.	M	Reporting Requirements		
20.6 h	Cost of call.	M	Reporting Requirements		
20.6 i	Manner in which the call started and ended.	M	Reporting Requirements		
20.7	The System allows User(s) to:		Reporting Requirements		
20.7 a	Print the currently displayed page of a report.	M	Reporting Requirements		
20.7 b	E-mail the currently displayed page of a report.	M	Reporting Requirements		
20.7 c	Export the currently displayed page of a report in various file formats (i.e., PDF, Excel, RTF, TXT, or TIFF).	M	Reporting Requirements		
20.7 d	View the call activities of each Telephone Instrument located within a particular Facility.	M	Reporting Requirements		
	ADDITIONAL RECORDED CALL FILE REQUIREMENTS				
21.0	All recorded calls comply with the following measures for recording and storing:		Record File Format		
21.0 a	Recorded call file format is encrypted as a .WAV and/or .MP3 file.	M	Record File Format		
21.0 b	Recorded call file format has standalone capabilities (not connected to the ITMS) for authenticating recorded call files as pass or fail. This feature is required for situations where validated audio files must be played in a court room, as evidence, or in any other place the ITMS is not available.	M	Record File Format		
21.0 c	Recorded call file format standalone versions are compatible with Windows.	M	Record File Format		
21.0 d	Standalone version is available in a manner of distribution identical to call recording retrieval an download.	M	Record File Format		
21.0 e	Recorded call file format can be accessed on Apple/MacOS operating systems for users with an Apple/Macintosh computer.	M	Record File Format		
21.1	Contractor's ICSS provides a server grade solution available via LAN with web-based graphical user interface and supports 20 simultaneous web-users at minimum.		Record File Format		
21.1 a	The server has the ability to record calls when not connected to the network (non web-based).	M	Record File Format		
	DIPMS				
22.0	Contractor's ICSS includes DIPMS that converts physical U.S. postal inmate mail into digital files.	M	DIPMS		
22.1	Contractor's DIPMS provides the following capabilities:		DIPMS		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
22.1 a	Contractor to print hard copies of all digitized mail for mail delivery to Sheriff and Probation Facilities.	M	DIPMS		
22.1 b	County staff to print the digitized mail.	M	DIPMS		
22.1 c	Digitized mail to be retrieved from an Inmate Telephone Instrument (e.g., Inmate Tablet Devices, wall-mounted Kiosks).	M	DIPMS		
22.2	Contractor's DIPMS is capable of receiving Inmate mail via the following:		DIPMS		
22.2 a	Contractor's processing center or P.O. Box for hard copy mail	M	DIPMS		
22.2 b	Contractor's public facing website that allows friends and family to upload digital copies of Inmate correspondence.	M	DIPMS		
22.3	Contractor's DIPMS is capable of handling up to 1,000 parcels of mail per day.	M	DIPMS		
22.4	Contractor's DIPMS provides a web-enabled dashboard, which supports:		DIPMS		
22.4 a	Drill through capability to display digital images.	M	DIPMS		
22.4 b	Sorting capabilities (e.g., Inmate Booking number, housing location).	M	DIPMS		
22.4 c	The ability to perform a print function.	M	DIPMS		
22.4 d	The ability to maintain a screening list for watchwords, phrases, persons of interest, housing locations, etc.	M	DIPMS		
22.4 e	The capability to track the status of all digitized mail (e.g., approved, held for review, rejected for failing the screening process).	M	DIPMS		
22.4 f	The creation of role-based accounts accessing the web-enabled dashboard, upon authorization by the concerned County Project Director.	M	DIPMS		
22.4 g	Inmates to view mail and the status of mail (e.g., receiving, processing, ready for viewing).	M	DIPMS		
22.4 h	The addition or removal of policies with regard to type of mail received at Facilities.	M	DIPMS		
22.4 i	On-demand reports for all types of mail.	M	DIPMS		
22.4 j	Investigative dashboard capabilities provide a search functionality that permits County investigators to perform keyword searches across all digitized mail.	M	DIPMS		
22.5	Contractor's dashboard includes the following features:		DIPMS		
22.5 a	Searchable: allows the County to search by Inmate Booking Number, date of receipt, date of birth, etc.	M	DIPMS		
22.5 b	Downloadable: allows the County to download all digitized scanned mail	M	DIPMS		
22.5 b-i	Digitized scanned mail captures all sides and contents, including but not limited to, Inmate name, Booking Number, Facility, sender name, and the digitization timestamp.	M	DIPMS		
22.5 c	Printing: allows the County to print digitized scanned mail in the same format as Contractor's output and is acessible for printing at a centralized-level Facility or a module-level Facility.	M	DIPMS		

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
22.5 d	Reporting: alows the County to generate reports on mail processing metrics, including but not limited to volume of mail processed, digitized time, and delivery time.	M	DIPMS		
	ITD				
	INTRODUCTION				
	This set of requirements is not exhaustive. Proposers must consider the following Functional Requirements as minimum requirements. An attempt has been made to provide an overview of the processes and procedures which, together with Exhibit A (SOW) of Appendix A (Sample Contract) of the RFP, describe in sufficient detail County Work requirements. For the purpose of this Exhibit J, reference to the ITD solution includes the tablet/mobile device, infrastructure, and software needed to deploy and support an ITD solution. Approval of all content requirements throughout must be Approved by LASD.				
	SYSTEM FEATURES REQUIREMENTS		**ITD**		
23.0	The ITD solution includes an Inmate User registration that allows Inmates to register with a booking number.	M	ITD		
23.1	The ITD solution is capable of capturing voice biometric at Inmate User Registration.	M	ITD		
23.2	The ITD solution automatically allows access to newly booked Inmates, who are moved between housing units, without County staff involvement.	M	ITD		
23.4	The ITD solution includes a fee notification statement prior to being granted use of the ITDs.	M	ITD		
23.5	The ITD solution requires each Inmate to agree and to accept terms and conditions of ITD Services prior to being granted use of the ITDs.	M	ITD		
	ITD FEATURES		**ITD**		
24.0	The ITD provides access to collection of free music, games and book content.	M	ITD		
24.1	The ITD provides access to unlimited streaming music with a library of various songs, including access to:		ITD		
24.1 a	Country music.	M	ITD		
24.1 b	Rap music.	M	ITD		
24.1 c	Rock music.	M	ITD		
24.1 d	Pop music.	M	ITD		
24.1 e	Other music genres.	M	ITD		
24.2	The ITD allows Inmates the ability to create music playlists in a personal library and to search for music by:		ITD		
24.2 a	Artist.	M	ITD		
24.2 b	Song.	M	ITD		
24.2 c	Album.	M	ITD		
24.3	The ITD provides unlimited digital reading services, such as eBooks in various types of titles and includes access to:		ITD		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
24.3 a	Fiction books.	M	ITD		
24.3 b	Non-fiction books.	M	ITD		
24.3 c	Self-help books.	M	ITD		
24.3 d	Other types of books.	M	ITD		
24.4	The ITD allows Inmates to search for books by:		ITD		
24.4 a	Author.	M	ITD		
24.4 b	Title.	M	ITD		
24.4 c	Subject.	M	ITD		
24.4 d	Language.	M	ITD		
24.5	The ITD allows Inmates to save books to a personalized book library.	M	ITD		
24.6	The ITD includes a bookmark capability which saves previous reading sessions.	M	ITD		
24.7	The ITD provides game services, with a library of various games, including access to:		ITD		
24.7 a	Sport games.	M	ITD		
24.7 b	Arcade games.	M	ITD		
24.7 c	Puzzle games.	M	ITD		
24.7 d	Educational games.	M	ITD		
24.8	The ITD provides unlimited access to Podcasts.	M	ITD		
24.9	The ITD provides communication services for phone calls and electronic messaging.	M	ITD		
24.10	The ITD provides unlimited free access to:		ITD		
24.10 a	Educational content, resources, and services such as videos and eBooks.	M	ITD		
24.10 b	Job and life skills content and services.	M	ITD		
24.10 c	Law library content.	M	ITD		
24.10 d	Daily newspaper (.pdf or equivalent).	M	ITD		
24.10 e	Utilities content (dictionary, calendar, calculator, etc.).	M	ITD		
24.10 f	Religious Material (Bible, Quran, etc.) content.	M	ITD		
24.10 g	Commissary Ordering.	M	ITD		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
24.11	The ITD provides unlimited free access to the County's integrated Grievance and Inmate Requests application content.	M	ITD		
24.12	The ITD provides unlimited free access to County orientation videos and Facility specific instructional videos.	M	ITD		
24.13	The ITD provides unlimited free access to PREA information: • Notices • Education • Reporting Procedures	M	ITD		
24.14	The ITD is preloaded with specifically designed content approved by the County.	M	ITD		
24.15	The ITD provides access to an Inmate Tablet User Guide with self-help instructions on how to use Tablet and applications, how to add or update content, and information on Inmate services and products provided.	M	ITD		
	ITD FUNCTIONAL REQUIREMENTS		**ITD**		
25.0	The ITD is configured to prevent the use of a camera/video.	M	ITD		
25.1	The ITD restricts Inmate-to-Inmate communications.	M	ITD		
25.2	The ITD does **not** include Bluetooth, internal/external speaker, Micro SD card slot, data USB port, removable parts such as batteries, or security screws.	M	ITD		
25.3	The ITD is charged using a power only port.	M	ITD		
25.4	The ITD is configured to only logon to the VDN.	M	ITD		
25.5	The ITD is configured to function in only specified locations.	M	ITD		
25.6	The ITD has a screen size of 7" or up to 10", at County's discretion.	M	ITD		
25.7	The ITD is equipped with a tamper proof casing made of clear material.	M	ITD		
25.8	The ITD is tamper-resistant and designed for a correctional facility to comply with ADA requirements.	M	ITD		
	SYSTEM INTEGRATION/INTERFACE REQUIREMENTS		**ITD**		
26.0	The ITD integrates with future County systems to provide services to Inmates via the ITD (e.g., the County's Inmate Grievances and Requests system).	M	ITD		
26.1	The ITD interfaces in real-time with the following County applications:		ITD		
26.1 a	RAJIS, using web services and/or automated program interfaces for retrieving and verifying Inmate information and Inmate location.	M	ITD		
26.1 b	JIMS – Trust Accounting module, in order to grant access to Inmate trust account/spendable balance information to verify funds are available for successful purchases.	M	ITD		
26.2	The ITD provides hyperlinks to a third-party commissary ordering system.	M	ITD		
26.3	The ITD solution identifies the Inmate's main number (unique finger print biometric identifier) through the interface with JIMS.	M	ITD		
26.4	The ITD solution debits in real-time the Inmate trust account for purchases made through the JIMS interface.	M	ITD		
26.5	The ITD solution identifies the Inmate booking number through the interface with RAJIS.	M	ITD		
26.6	The ITD solution verifies the Inmate's voice print through the interface with County's AFIS.	M	ITD		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

Req #	Requirement	M/O	Category	B/C/D/X	Comments - Detailed discussion of how the proposed Solution meets the Requirement
26.7	The ITD solution interacts with JIMS Trust Accounting System to retrieve Inmate's:		ITD		
26.7 a	Trust account status information active/inactive to approve for purchases.	M	ITD		
26.7 b	Indigent status (obligation) information to approve for purchases.	M	ITD		
26.7 c	Restitution status (obligation) information to approve for purchases.	M	ITD		
26.7 d	*Pro-per* status (obligation) information to allow for purchases.	M	ITD		
26.7 e	Account balances to allow for purchases.	M	ITD		
	SYSTEM ADMINISTRATIVE REQUIREMENTS		**ITD**		
27.0	The ITD Administrators are provided with access to monitor ITD activity and have the capacity to shut ITD down (disable) when necessary.	M	ITD		
27.1	The ITD Administrators have the capability to:		ITD		
27.1 a	Upload documents electronically for information distribution to Inmates. Capability must be enterprise-wide or local Facility based.	M	ITD		
27.1 b	Restrict Inmate ordering content for individual Inmates based on the following:		ITD		
27.1 b-i	By category.	M	ITD		
27.1 b-ii	By housing location.	M	ITD		
27.1 b-iii	By discipline type.	M	ITD		
27.2	The ITD User authentication for Sheriff employees is integrated with Active Directory.	M	ITD		
	SECURITY REQUIREMENTS		**ITD**		
28.0	The ITD is designed to only connect to designated wireless networks (VDN).	M	ITD		
28.1	Inmates are not able to access any features of the ITD that are not authorized for Inmate use or access.	M	ITD		
28.2	The ITD is equipped with centrally managed anti-malware software.	M	ITD		
28.3	The ITD is centrally managed using a MDM system.	M	ITD		
28.4	The ITD offers appropriate User authentication for the Inmates. This must be approved by the LASD's designated Data Security Officer.	M	ITD		
	SYSTEM TECHNICAL SUPPORT		**ITD**		
29.0	The ITD Technical support is provided on-site during business hours and remote support 24x7x365.	M	ITD		
29.1	The ITD Technical support for issues with system security, performance, connectivity and outages is available on-site 24x7x365.	M	ITD		
29.2	The ITD solution Technical support for all proposed entertainment products is available via Web-Based service tracking system, email and/or telephone call with live operator 24x7x365.	M	ITD		

EXHIBIT J
INMATE COMMUNICATION SYSTEM AND SERVICES (ICSS) SOLUTION REQUIREMENTS

ACRONYM	DEFINITION
.MP3	MPEG-1 Audio Layer 3
.WAV	Waveform Audio File Format
ADA	Americans with Disabilities Act
AES	Advanced Encryption Standard
API	Application Program Interface
DIPMS	Digitized Inmate Postal Mail Services
FCC	Federal Communications Commission
GUI	Graphical User Interface
ICSS	Inmate Communication System and Services
IP	Internet Protocol
ITD	Inmate Tablet Device
ITMS	Inmate Telephone Management System
ITS	Inmate Telephone System
JIMS	Jail Information Management System
LAN	Local Area Network
MDM	Mobile Device Management
NEC	National Electrical Code
PDF	Portable Document Format
PREA	Prison Rape Elimination Act
RAJIS	Replicated Automated Justice Information System
RFP	Request for Proposals
RTF	Rich Text Format
SD	Secure Digital
SDN	Sheriff's Data Network
SOW	Statement of Work
TDD	Telecommunications Devices for the Deaf
TIFF	Tagged Image File Format
TXT	Text Only Format
UL	Underwriters Laboratories
UPS	Uninterruptible Power Supply
VDN	Vector Directory Number

CONTRACT DISCREPANCY REPORT

CONTRACTOR RESPONSE DUE BY:

Date:		**Contractor Response Received:**
Contractor:	**Contract No.**	**County Project Manager:**
Contact Person:	**Telephone:**	**County Project Manager Signature:**
Email:		**Email:**

A contract discrepancy(s) is specified below. Contractor must take corrective action and respond back to the County personnel identified above by the date required. Failure to take corrective action or respond to this Contract Discrepancy Report by the date specified may result in the deduction of damages.

No.	Contract Discrepancy	Contractor's Response*	County Use Only		
			Date Correction Due	Date Completed	Approved
1					
2					
3					

***Use additional sheets if necessary**

_____ _____

Contractor's Representative Signature ***Date Signed***

Additional Comments: