LOS ANGELES COUNTY
REGIONAL PARK AND
OPEN SPACE DISTRICT

1000 S. Fremont Avenue
Unit #40 Building A-9 East
Ground Floor
Alhambra, CA 91803
(626) 588-5060

RPOSD.LACounty.gov
info@RPOSD.LACounty.gov

November 6, 2024

The Honorable Board of Directors
County of Los Angeles
Regional Park and Open Space District
303 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Directors:

APPROVAL OF SOLE SOURCE AMENDMENT TO THE GRANTS MANAGEMENT SYSTEM AGREEMENT WITH DULLES TECHNOLOGY PARTNERS, INC. FOR CONTINUED MAINTENANCE AND SERVICING (ALL SUPERVISORIAL DISTRICTS - 3 VOTES) CIO RECOMMENDATION: APPROVE (X)

SUBJECT

The Los Angeles County Regional Park and Open Space District (RPOSD) requests delegated authority to approve a sole source Amendment to an existing Agreement with Dulles Technology Partners, Inc. (Dulles), to extend the term and allow for the continued hosting, maintenance, and servicing of the Grants Management System (GMS), which automates grant data collection, reporting, and tracking of RPOSD's Proposition A and Measure A grant program services.

IT IS RECOMMENDED THAT THE BOARD:

1. Find that the proposed actions are not a project under the California Environmental Quality Act for the reasons stated in this Board letter and the record.

2. Delegate authority to the Director of the Department of Parks and Recreation, acting as the Director of RPOSD, or her designee, to execute a sole source Amendment (Attachment I) with Dulles to extend the Agreement term for an additional six (6) months to June 30, 2025; and twelve (12) additional month-to-month optional extensions up to June 30, 2026, as needed. The original contract sum of $370,000 remains unchanged.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

RPOSD is a California Special District established pursuant to Section 5506.9 of the Public Resource Code, with the Los Angeles County (County) Board of Supervisors (Board) acting as RPOSD's governing body. To maintain transparency and accountability to the public and fairness to its various grant recipients, RPOSD operates as an independent agency of the County, with the District Administrator reporting directly to the Director of the Department of Parks and Recreation (DPR), acting as RPOSD's Director (Director).

On October 2, 2018, your Board approved the Sole Source Agreement (Agreement) with Dulles for the development, licensing, implementation, on-going hosting, maintenance, and servicing of the GMS system. The first online grant applications for RPOSD funds went live in May 2019.

As RPOSD pursues a new long-term replacement system, there is an operational need to continue utilizing the GMS system for automated grant data collection, reporting, and tracking of grantee funding and program management. To ensure a seamless transition and avoid service disruptions, it is essential to extend the Agreement. This extension will cover the period necessary to implement the new system, train staff, and ensure a smooth transition without interrupting grant services.

The Agreement will expire on December 31, 2024. As a result of cost-saving measures, there are available funds within the existing budget to fund the extension period. As a result, no additional funding is required, and the maximum contract sum remains at $370,000, as previously approved by your Board in 2018.

CONTRACTING PROCESS

On October 2, 2018, your Board approved the Agreement with Dulles for an initial term of three years.

Amendment No. 1 to the Agreement was executed on July 27, 2020, pursuant to delegated authority to RPOSD, realigning the pricing schedule and deliverables identified within the Agreement to streamline invoice processing.

Amendment No. 2 to the Agreement was authorized by your Board on August 10, 2021, extending the Agreement term from September 30, 2021, through December 31, 2024, or until the Contract Sum was exhausted, whichever occurred first.

On August 22, 2024, RPOSD released a Request for Proposals (RFP) to solicit proposals from qualified bidders to acquire and implement a Commercial Off-the-Shelf modular, cloud-based, enterprise solution to replace and modernize the existing on-line GMS system. A new agreement must be established prior to the conclusion of the current Agreement. The overlapping timeframe is necessary to develop and implement a new

system, migrate existing data, properly train staff, develop online applications and grant related forms, and educate users prior to launch.

In compliance with Board Policy 6.020, Chief Information Office Board Letter Approval, the Chief Information Office has reviewed the information technology (IT) components of this request and recommends approval. The CIO determined this recommended action does not include any IT items or services that would necessitate a formal written CIO analysis.

In accordance with the Board's Policy Number 5.100, Sole Source Contracts, the Sole Source Checklist is attached (Attachment II). The Notice of Intent to amend the sole source Agreement with Dulles and extend the term of the Agreement was delivered to your Board on July 24, 2024 (Attachment III).

Implementation of Strategic Plan Goals

The recommended actions align with the following strategic goals of the County's Strategic Plan, specifically: North Star 3 – Realize Tomorrow's Government Today; Data-Driven Decision Making; Strategy E (i) – Facilitate Data Sharing; Flexible and Efficient Infrastructure; Strategy F (iii) – Technology Advancement/Digital Divide.

FISCAL IMPACT/FINANCING

The Amendment will not impact fiscal resources or require additional funding. The total contract sum will remain at $370,000. Non-expended funds will be used for continued hosting, maintenance, and support through the extension period, including the optional monthly extensions, if exercised by RPOSD.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

RPOSD is authorized to enter into agreements and/or contracts for goods and/or services under State of California Public Resources Code Section 5500 et seq., subject to delegated authority by the Board.

Pursuant to the Change Notices and Amendments section of the Agreement, the Agreement may be amended by further written agreement between the parties. Any such modification shall not be effective and until executed by the contractor and in the case of County, until approved by your Board. The recommended action will allow the Director, or her designee, to execute an amendment to extend the Agreement term. The Amendment updates the terms of the Agreement to include all current Board required provisions. County Counsel has reviewed and approved the Amendment as to form.

ENVIRONMENTAL DOCUMENTATION

The proposed approval of the Agreement amendment to extend hosting, maintenance, and servicing of the GMS system is not subject to the California Environmental Quality Act (CEQA) because they are activities that are excluded from the definition of a project by section 21065 of the Public Resources Code and Section 15378 (b) of the State CEQA Guidelines. The proposed action to extend the existing Agreement is an organizational or administrative activity of government which will not result in direct or indirect physical changes to the environment.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Extending the term of the Agreement will have no negative impact on current services or projects. The extension will ensure uninterrupted service delivery and continued use of the GMS system throughout the extension period.

CONCLUSION

Upon your approval of the recommended actions, the Director of RPOSD, or her designee, will proceed to execute the Agreement amendment. Your Board's approval of the Amendment will allow RPOSD to continue implementing grant making programs effectively while a comprehensive solicitation for a future online, paperless grants management system is completed.

Please instruct the Executive Officer-Clerk of the Board to return one adopted copy of this action to the Regional Park and Open Space District.

Respectfully submitted,

Norma E. García-González
Director

Reviewed By:

Peter Loo
Chief Information Officer

NEGG:CA:mrt

Attachments

c: Chief Executive Officer
County Counsel
Executive Officer, Board of Supervisors

LOS ANGELES COUNTY
REGIONAL PARK AND
OPEN SPACE DISTRICT

1000 S. Fremont Avenue, Unit #40
Building A-9 East, Ground Floor
Alhambra, CA 91803
(626) 588-5060

RPOSD.LACounty.gov

AMENDMENT NO. 3 TO AGREEMENT

WITH DULLES TECHNOLOGY PARTNERS, INC
FOR ENTERPRISE GRANTS MANAGEMENT SYSTEM

THIS AMENDMENT NO. 3 to the Agreement is made and entered into this ____ day of _____ 2024, by and between the LOS ANGELES COUNTY REGIONAL PARK AND OPEN SPACE DISTRICT (hereinafter referred to as "RPOSD") and **DULLES TECHNOLOGY PARTNERS, INC.** (hereinafter referred to as "CONTRACTOR").

RECITALS:

WHEREAS, Agreement ("Contract") was entered into between RPOSD and the CONTRACTOR on October 9, 2018, for the provision of information technology support services – Enterprise Grants Management System ("Services") for an initial period of three (3) years commencing October 2, 2018 through September 30, 2021; and

WHEREAS, Amendment No. 1 was executed on July 27, 2020, pursuant to delegated authority to RPOSD, to realign the pricing schedule and deliverables identified within the Agreement and streamline the invoice processing.

WHEREAS, Amendment No. 2 was executed on August 18, 2021, by your Board for the extension of the Contract term from September 30, 2021, through December 31, 2024, or until the Contract Sum was exhausted, whichever occurred first.

WHEREAS, RPOSD and Contractor wish to amend the Contract to extend the term for an additional six (6) months, with twelve (12) additional month-to-month optional extensions to be exercised in RPOSD's sole discretion.

WHEREAS, Section 8.1 of the Contract provides that RPOSD may require the addition and/or change of certain terms and conditions required by RPOSD during the term of the Contract; and an amendment to the Contract must be executed between the Contractor and RPOSD for any change affecting the scope of work, term, contract sum, payments, or any term or condition of the Contract; and

WHEREAS, RPOSD requires amendments to the following provisions: 1) Assignments and Delegation/Merges or Acquisitions; 2) Contractor's Acknowledgement of County's Commitment to Safely Surrendered Baby Law; 3) Facsimile Representations; 4) Notice to Employees Regarding the Safely Surrendered Baby Law; 5) Public Records Act; 6)

Termination for Improper Consideration; 7) Compliance with the County Policy of Equity; 9) Exhibit B-1; and

WHEREAS, RPOSD mandates the addition of the following provisions: 1) Injury and Illness Prevention Program; and 2) Campaign Contribution Prohibition Following Final Decision in Contract Proceeding.

NOW, THEREFORE, in consideration of the mutual undertakings herein, RPOSD and Contractor agree that the Contract be amended as follows:

1. Section 4.2, TERM OF CONTRACT is hereby deleted in its entirely and replaced as follows:

4 TERM OF CONTRACT

4.2 The Contract Term shall commence on October 2, 2018, and terminate on June 30, 2025, unless otherwise extended. RPOSD, in its sole discretion, may extend Contract on a month-to-month basis for up to twelve (12) additional months by providing written notice of said extension to Contractor.

2. Section 8.2, ASSIGNMENT AND DELEGATION/MERGERS OR ACQUISITIONS, is hereby deleted in its entirety and replaced as follows:

8.2 Assignment and Delegation/Mergers or Acquisitions

8.2.1 The Contractor must notify RPOSD of any pending acquisitions/mergers of its company unless otherwise legally prohibited from doing so. If the Contractor is restricted from legally notifying RPOSD of pending acquisitions/mergers, then it should notify RPOSD of the actual acquisitions/mergers as soon as the law allows and provide to RPOSD the legal framework that restricted it from notifying RPOSD prior to the actual acquisitions/mergers.

8.2.2 The Contractor must not assign, exchange, transfer, or delegate its rights or duties under this Contract, whether in whole or in part, without the prior written consent of RPOSD, in its discretion, and any attempted assignment, delegation, or otherwise transfer of its rights or duties, without such consent will be null and void. For purposes of this paragraph, RPOSD consent will require a written Amendment to the Contract, which is formally approved and executed by the parties. Any payments by RPOSD to any approved delegate or assignee on any claim under this Contract will be deductible, at RPOSD's sole discretion, against the claims, which the Contractor may have against RPOSD.

8.2.3 Any assumption, assignment, delegation, or takeover of any of the Contractor's duties, responsibilities, obligations, or

performance of same by any person or entity other than the Contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever without RPOSD's express prior written approval, will be a material breach of the Contract which may result in the termination of this Contract. In the event of such termination, RPOSD will be entitled to pursue the same remedies against Contractor as it could pursue in the event of default by Contractor.

3. Section 8.13, CONTRACTOR'S ACKNOWLEDGMENT OF COUNTY'S COMMITMENT OT SAFELY SURRENDERED BABY LAW, is hereby deleted in its entirety and replaced as follows:

8.13 Contractor's Acknowledgement of County's Commitment to Safely Surrendered Baby Law

The Contractor acknowledges that the County and RPOSD place a high priority on the implementation of the Safely Surrendered Baby Law. The Contractor understands that it is the County's policy to encourage all County contractors to voluntarily post the County's poster, Exhibit G (Safely Surrendered Baby Law) in a prominent position at the Contractor's place of business. The Contractor will also encourage its subcontractors, if any, to post this poster in a prominent position in the subcontractor's place of business. Information and posters for printing are available at https://lacounty.gov/residents/family-services/child-safety/safe-surrender/.

4. Section 8.18, FACSIMILE REPRESENTATIONS, is hereby deleted in its entirety.

5. Section 8.33, NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW, is here by deleted in its entirety and replaced as follows:

8.33 Notice to Employees Regarding the Safely Surrendered Baby Law

The Contractor must notify and provide to its employees, and will require each subcontractor to notify and provide to its employees, information regarding the Safely Surrendered Baby Law, its implementation in Los Angeles County, and where and how to safely surrender a baby. The information is set forth in Exhibit G (Safely Surrendered Baby Law) of this Contract. Additional information is available at https://lacounty.gov/residents/family-services/child-safety/safe-surrender/.

6. Section 8.36, PUBLIC RECORDS ACT, is hereby deleted in its entirety and replaced as follows:

8.36 Public Records Act

8.36.1 Any documents submitted by the Contractor; all information

obtained in connection with the RPOSD'S right to audit and inspect the Contractor's documents, books, and accounting records pursuant to Paragraph 8.38 (Record Retention and Inspection-Audit Settlement) of this Contract; as well as those documents which were required to be submitted in response to the Request for Proposals (RFP) used in the solicitation process for this Contract, become the exclusive property of RPOSD. All such documents become a matter of public record and will be regarded as public records. Exceptions will be those elements in the California Government Code Section 7921 et seq. (Public Records Act) and which are marked "trade secret", "confidential", or "proprietary". RPOSD will not in any way be liable or responsible for the disclosure of any such records including, without limitation, those so marked, if disclosure is required by law, or by an order issued by a court of competent jurisdiction.

8.36.2 In the event RPOSD is required to defend an action on a Public Records Act request for any of the aforementioned documents, information, books, records, and/or contents of a proposal marked "trade secret", "confidential", or "proprietary", the Contractor agrees to defend and indemnify RPOSD from all costs and expenses, including reasonable attorney's fees, in action or liability arising under the Public Records Act.

7. Section 8.71, COMPLIANCE WITH THE COUNTY POLICY OF EQUITY, is hereby deleted and replaced as follows:

8.57 Compliance with the County Policy of Equity

The Contractor acknowledges that the County and RPOSD take their commitment to preserving the dignity and professionalism of the workplace very seriously, as set forth in the County Policy of Equity (CPOE) (https://ceop.lacounty.gov/). The Contractor further acknowledges that the County and RPOSD strive to provide a workplace free from discrimination, harassment, retaliation and inappropriate conduct based on a protected characteristic, and which may violate the CPOE. The Contractor, its employees and subcontractors acknowledge and certify receipt and understanding of the CPOE. Failure of the Contractor, its employees or its subcontractors to uphold the County's and RPOSD's expectations of a workplace free from harassment and discrimination, including inappropriate conduct based on a protected characteristic, may subject the Contractor to termination of contractual agreements as well as civil liability.

8. Paragraph 8.75 is hereby added as follows:

Injury and Illness Prevention Program

Contractor will be required to comply with the State of California's Cal OSHA's regulations. California Code of Regulations Title 8 Section 3203 requires all California employers to have a written, effective Injury and Illness Prevention

Program (IIPP) that addresses hazards pertaining to the particular workplace covered by the program.

9. Paragraph 8.76 is hereby added as follows:

Campaign Contribution Prohibition Following Final Decision in Contract Proceeding
Pursuant to Government Code Section 84308, Contractor and its Subcontractors, are prohibited from making a contribution of more than $250 to a County officer for twelve (12) months after the date of the final decision in the proceeding involving this Contract. Failure to comply with the provisions of Government Code Section 84308 and of this paragraph, may be a material breach of this Contract as determined in the sole discretion of RPOSD.

10. Exhibit B1 – Pricing Schedule and Prior Payments, is hereby deleted in its entirety and replaced with Exhibit B2 attached herein.

11. Exhibit P – Information Security and Privacy Requirements is deleted in its entirely and replaced as follows with Exhibit P1 attached herein.

12. Except as modified by AMENDMENTS 1 and 2, all terms, conditions, requirements, and specifications of this Contract shall remain in full force and effect.

IN WITNESS WHEREOF, RPOSD has caused this AMENDMENT 3 to be subscribed by the Director of the Department of Parks and Recreation, acting as the Director of RPOSD, or her designee, and CONTRACTOR by its duly authorized officer, as of the day, month, and year first written above.

CONTRACTOR,
DULLES TECHNOLOGY PARTNERS, INC.

By: _____

Name: Tom Nyilasi

Title: Principal

Date: _____

LOS ANGELES COUNTY REGIONAL PARK AND OPEN SPACE DISTRICT

By: _____

Name: Christina Angeles

Title: District Administrator

Date: _____

Approved as to Form:

COUNTY COUNSEL
Dawyn R. Harrison

By: _____

Name: Parjack Ghaderi

Title: Principal Deputy County Counsel

Date: _____

Exhibit B2 – Pricing Schedule and Prior Payments

Deliverable/ Task Category/ Description Available Budget	Allocated	Expended	Available
Requirements/ Project Organization	$17,500.00	$17,500.00	**$0.00**
System Configuration	$60,500.00	$60,500.00	**$0.00**
Training	$19,000.00	$19,000.00	**$0.00**
Data Migration	$25,000.00	$25,000.00	**$0.00**
Validation	$20,000.00	$20,000.00	**$0.00**
Travel	$0.00	$0.00	**$0.00**
Hosting, Maintenance and Support	$206,850.00	$171,750.00	**$35,100.00**
Contingency	$21,150.00	$0.00	**$21,150.00**
Total:	$ 370,000.00	$ 313,750.00	**$ 56,250.00**

INFORMATION SECURITY AND PRIVACY REQUIREMENTS EXHIBIT

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 the 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 the Contractor before the Effective Date of the Contract and maintained throughout the term of the 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 the 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 the 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 shall 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.** The Contractor shall 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 shall 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.

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

The Contractor's Information Security Program shall:

- 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 the Contractor.

b. **Privacy Program**. The Contractor shall 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. The Contractor's Privacy Program shall 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. The Contractor's Privacy Policies, guidelines, and procedures shall 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. The Contractor's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

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

The Contractor's Privacy Program shall include:

- A Privacy Program framework that identifies and ensures that the 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 shall retain exclusive rights and ownership thereto. County Information shall not be used by the Contractor for any purpose other than as required under this Contract, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The 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, the 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 the 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. The 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**

The Contractor may use County Information only as necessary to carry out its obligations under this Contract. The Contractor shall 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**

The Contractor shall 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.** The 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.** The 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, the Contractor shall 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, the 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. The Contractor shall not disclose or publish any County NPI and material received or used in performance of this Contract. This obligation is perpetual.
d. **Individual Requests.** The Contractor shall acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided

under applicable federal or state laws. The Contractor shall 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 the Contractor involving County Information, the Contractor shall notify the County within five (5)calendar days and the County will coordinate an appropriate response, which may include instructing the Contractor to assist in fulfilling the request. Similarly, if the Contractor receives a privacy or security complaint from an individual regarding County Information, the Contractor shall 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**. The Contractor shall not retain any County Information for any period longer than necessary for the Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. **CONTRACTOR EMPLOYEES**

The Contractor shall 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, the Contractor shall 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 shall be at the expense of the Contractor, regardless of whether the member of the Contractor's staff passes or fails the background investigation. The Contractor, in compliance with its legal obligations, shall 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.

The Contractor shall 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 the Contractor.

The Contractor shall supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks, and Threats. The 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:** The Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

The Contractor shall have an established set of procedures to ensure the 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, the 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 shall also apply to all Subcontractors and third parties. The Contractor or third party shall 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 the 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) the Contractor shall 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.

The Contractor shall 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 shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, the 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.

The Contractor will encrypt County Information transmitted on networks outside of the 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, the Contractor shall 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 shall 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**

The Contractor shall 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 shall (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 the 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, the Contractor shall 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, the Contractor shall 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, the Contractor shall return all hardware, if any, provided by the County to the Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. **Method of Destruction**. The Contractor shall 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. The 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 the 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**

The Contractor shall: (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.

The 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 the Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups shall 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 the Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements shall apply to back-up media stored by the Contractor at off-site facilities.

The Contractor shall 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 shall 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. The 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. The Contractor shall 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, the Contractor shall 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, the Contractor shall:

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 shall 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:
Jeff Aguilar
Chief Information Security Officer 320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 253-5600

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

Departmental Information Security Officer:
Ken Ta
Dpt. Information Security Officer 1000 S. Fremont Ave. Unit #40
Alhambra, CA 91803
(626) 588-5020

Ken Ngoy (ADISO)
Assistant Dpt. Information Security Officer
1000 S. Fremont Ave. Unit #40
Alhambra, CA 91803
(626) 588-5011

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 the Contractor, and unless prohibited by law, the Contractor shall 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 the 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, the Contractor shall 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 the Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. **NON-EXCLUSIVE EQUITABLEREMEDY**

The 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 shall constitute a material breach of this Contract and be grounds for immediate termination of this Contract in the exclusive discretion of the County.

16. **AUDITANDINSPECTION**

a. **Self-Audits.** The Contractor shall 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.

The Contractor shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. The Contractor shall 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 the Contractor that contains any County Information, the Contractor shall promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Contractor's Information systems, products, and services, and the corresponding steps taken by the Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section shall 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, shall have the right to audit the 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 the Contractor shall complete a questionnaire regarding Contractor's Information Security and/or program. The County shall pay for the County requested audit unless the auditor finds that the Contractor has materially breached this Exhibit, in which case the Contractor shall 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 shall be conducted during the Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the 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. The Contractor shall 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 shall extend to any regulators with oversight of the County. The Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

When not prohibited by regulation, the Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by

the Contractor or a third party; and (ii) corrective actions or modifications, if any, the Contractor will implement in response to such audits.

17. **CYBER LIABILITY INSURANCE**

Contractor shall secure and maintain cyber liability insurance coverage in the manner prescribed in this section unless the Contract prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this section. The Contractor shall secure and maintain cyber liability insurance coverage with limits of at least $ 2 million per occurrence and in the aggregate during the term of the Contract, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Contract. The Contractor shall add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. **PRIVACY AND SECURITY INDEMNIFICATION**

In addition to the indemnification provisions in the Contract, the 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:

- The Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;
- The 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 the 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 shall 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 shall 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 shall 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.

ADDENDUM A: SOFTWARE AS A SERVICE (SaaS)

a. **License:** Subject to the terms and conditions set forth in this Contract, including payment of the license fees by to the Contractor, the Contractor hereby grants to County a non-exclusive, non- transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of this Contract to enable the County to use the full benefits of the SaaS and achieve the purposes stated herein.

b. **Business Continuity:** In the event that the Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed, or otherwise limited in functionality in a way that affects the County's use of the SaaS, The Contractor shall immediately and within twenty- four (24) hours implement the Contractor's Business Continuity Plan, consistent with Section 12 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that the Contractor can continue to provide full functionality of the SaaS as described in the Contract.

   The Contractor will indemnify the County for any claims, losses, or damages arising out of the County's inability to use the SaaS consistent with the Contract and Section 18 PRIVACY AND SECURITY INDEMNIFICATION.

   The Contractor shall include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

   In the event that the SaaS is interrupted, the County Information may be accessed and retrieved within two (2) hours at any point in time. To the extent the Contractor hosts County Information related to the SaaS, the Contractor shall create daily backups of all County Information related to the County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in this Contract and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: The Contractor agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which the Contractor initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Contractor's other customers.

   During the term of this Contract, the Contractor shall promptly notify the County of any available updates, enhancements or newer versions of the SaaS and within thirty (30) Days update or provide the new version to the County. The Contractor shall provide any accompanying documentation in the form of new or revised documentation necessary to enable the County to understand and use the enhanced, updated, or replaced SaaS.

   During the Contract term, the Contractor shall not delete or disable a feature or functionality of the SaaS unless the Contractor provides sixty (60) Days advance notice and the County

provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, the County shall have the sole discretion whether to accept such replacement. The replacement shall be at no additional cost to the County. If the Contractor fails to abide by the obligations in this section, the County reserves the right to terminate the Contract for material breach and receive a pro-rated refund.

d. **Location of County Information:** The Contractor warrants and represents that it shall store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. **Audit and Certification:** The Contractor agrees to conduct an annual System and Organization Controls (SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. The Contractor shall have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and the Contractor's plan for addressing or resolving the audit findings shall be shared with County's Chief Information Security Officer within ten (10) business days of the Contractor's receipt of the audit results. The Contractor agrees to provide County with the current audit certifications upon request.

f. **Services Provided by a Subcontractor:** Prior to the use of any Subcontractor for the SaaS under this Contract, the Contractor shall notify County of the proposed subcontractor(s) and the purposes for which they may be engaged at least thirty (30) Days prior to engaging the Subcontractor and obtain written consent of the County's Contract Administrator.

g. **Information Import Requirements at Termination:** Within one (1) Day of notification of termination of this Contract, the Contractor shall provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. **Termination Assistance Services:** During the ninety (90) Day period prior to, and/or following the expiration or termination of this Contract, in whole or in part, the Contractor agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

    i. Developing a plan for the orderly transition of the terminated or expired SaaS from the Contractor to a successor;
    ii. Providing reasonable training to County staff or a successor in the performance of the SaaS being performed by the Contractor;
    iii. Using its best efforts to assist and make available to the County any third-party services then being used by the Contractor in connection with the SaaS; and
    iv. Such other activities upon which the Parties may reasonably agree.

ADDENDUM B: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in this Contract, the Contractor shall ensure the following provisions and security controls are established for any and all Systems or Hardware provided under this contract.

a. **Inventory:** The Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under this Contract. The Contractor must be able to provide such management records to the County at inception of the contract and upon request.

b. **Access Control:** The Contractor agrees to manage access to all Systems or Hardware covered under this contract. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing Systems or Hardware under this Contract, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of this Contract, the Contractor must document their access control plan for Systems or Hardware covered under this Contract and provide such plan to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) for review and approval. The Contractor must modify and/or implement such plan as directed by the DISO and CISO.

c. **Operating System and Equipment Hygiene:** The Contractor agrees to ensure that Systems or Hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within ninety (90) Days of the release of such updates, upgrades, or patches. The Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason the Contractor cannot do so within ninety (90) Days, the Contractor must provide a Risk assessment to the County's Chief Information Security Officer (CISO).

d. **Vulnerability Management:** The Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this Contract. If such vulnerabilities cannot be addressed, The Contractor must provide a Risk assessment to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO). The County's CISO must approve the Risk acceptance and the Contractor accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.

e. **Media Encryption:** Throughout the duration of this Contract, the Contractor will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with Systems and Hardware provided under this Contract in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by the County's Chief Information Security Officer (CISO).

f. **Malware Protection:** The Contractor will provide and maintain industry-standard endpoint antivirus and antimalware protection on all Systems and Hardware as approved or required by the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) to ensure provided hardware is free, and remains free of malware. The Contractor agrees to provide the County documentation proving malware protection status upon request.

SOLE SOURCE CHECKLIST

Department Name: Department of Parks and Recreation – Regional Park and Open Space District

☐ New Sole Source Contract

☐ Existing Sole Source Contract Date Sole Source Contract Approved: _____

Check (✓)	JUSTIFICATION FOR SOLE SOURCE CONTRACTS **Identify applicable justification and provide documentation for each checked item.**
	➢ Only one bona fide source (monopoly) for the service exists; performance and price competition are not available. Monopoly is an "*Exclusive control of the supply of any service in a given market. If more than one source in a given market exists, a monopoly does not exist* ."
	➢ Compliance with applicable statutory and/or regulatory provisions.
	➢ Compliance with State and/or federal programmatic requirements.
	➢ Services provided by other public or County-related entities.
	➢ Services are needed to address an emergent or related time-sensitive need.
	➢ The service provider(s) is required under the provisions of a grant or regulatory requirement.
	➢ Services are needed during the period required to complete a solicitation for replacement services; provided services are needed for no more than 12 months from the expiration of an existing contract which has no available option periods.
✓	➢ Maintenance and support services are needed for an existing solution/system during the time to complete a solicitation for a new replacement solution/system; provided the services are needed for no more than 24 months from the expiration of an existing maintenance and support contract which has no available option periods.
✓	➢ Maintenance service agreements exist on equipment which must be serviced by the original equipment manufacture or an authorized service representative.
	➢ It is more cost-effective to obtain services by exercising an option under an existing contract.
	➢ It is in the best economic interest of the County (e.g., significant costs to replace an existing system or infrastructure, administrative cost savings and excessive learning curve for a new service provider, etc.) In such cases, departments must demonstrate due diligence in qualifying the cost-savings or cost-avoidance associated with the best economic interest of the County.

_____ _____

Chief Executive Office Date

Attachment III

LOS ANGELES COUNTY
REGIONAL PARK AND
OPEN SPACE DISTRICT

1000 S. Fremont Avenue
Unit #40 Building A-9 East
Ground Floor
Alhambra, CA 91803
(626) 588-5060

RPOSD.LACounty.gov
info@RPOSD.LACounty.gov

July 24, 2024

TO: Supervisor Lindsey P. Horvath, Chair
Supervisor Hilda L. Solis
Supervisor Holly J. Mitchell
Supervisor Janice Hahn
Supervisor Kathryn Barger

FROM: Norma E. García-González
Director, Regional Park and Open Space District

SUBJECT: **ADVANCE NOTICE OF INTENT TO AMEND THE SOLE SOURCE GRANTS MANAGEMENT SYSTEM AGREEMENT WITH DULLES TECHNOLOGY PARTNERS, INC. TO EXTEND THE TERM OF SERVICE**

This is to provide the Board advanced notification that the Los Angeles County Regional Park and Open Space District (RPOSD) intends to negotiate a sole source amendment, in compliance with Board Policy 5.100, to extend an existing agreement with Dulles Technology Partners, Inc. (Dulles) for an anticipated additional six (6) months, with up to nine (9) additional month to month optional extensions, for provisioning of its online, paperless Grants Management System (GMS) which automates grant data collection, reporting, and tracking of the District's Measure A grant program services.

The current Sole Source Agreement (Agreement) will expire on December 31, 2024. The sole source amendment will allow for continued operation of the GMS system and enable RPOSD enough time to complete a Request for Proposal (RFP) solicitation, to award, negotiate and execute a successor agreement, and to implement a long-term replacement system. Development of the solicitation is underway, and RFP is expected to be released in the next few weeks.

There will be no impact to the County General Fund as the funding for the system is provided by the Measure A special tax.

Background

On October 2, 2018, your Board approved the Agreement between RPOSD and Dulles for an online, paperless GMS system. The Agreement was in the amount of $370,000

for the development, licensing, implementation, hosting, maintenance, and servicing of the GMS.

On August 2021, due to cost-saving practices, RPOSD amended the Agreement solely to extend the term and thus allow for the utilization of non-expended allocations for the continued hosting, maintenance, and servicing of the GMS. The Agreement is set to expire on December 31, 2024.

Justification

As RPOSD pursues a new long-term replacement system, there is an operational need to continue utilizing the GMS system for automated grant data collection, reporting, and tracking of grantee funding and program management. If the GMS system was to terminate before a new system is solicited, this would disrupt services to park agencies as it would be difficult to reimburse grantees would for maintenance and servicing or completed grant projects. To effectively continue a seamless online system, RPOSD requires an extension of the Agreement, prior to entering into an agreement for the replacement system. The overlapping timeframe is necessary to develop and implement a new system, properly train staff, develop online applications, grant related forms, and educate users prior to launch.

Should a new vendor system be selected, RPOSD would require Dulles' assistance to plan and execute the transition to the new system that minimizes disruptions to RPOSD's operations and the delivery of services. Dulles would support the successful migration of grant data from the existing GMS system to the new system, ensuring that data integrity and security are maintained throughout the migration process. Additionally, Dulles' GMS system would serve as backup in case the new system transition encounters unexpected changes.

Conclusion

RPOSD will proceed with the extension amendment with Dulles as described herein, unless otherwise instructed by your Board. If no objection is received from the Board, we will work with County Counsel to prepare an amendment with Dulles and return to the Board for approval of the amendment.

If you have any questions, please contact me at (626) 588-5373 or your staff may contact Christina Angeles, District Administrator, Regional Park and Open Space District at cangeles@rposd.lacounty.gov or (626) 588-5060.

NEGG:CA:MRT:ee

c: Chief Executive Officer
County Counsel
Executive Officer, Board of Supervisors