LOS ANGELES COUNTY
AGING AND DISABILITIES DEPARTMENT
INVITATION FOR BID (IFB)
HEALTH INSURANCE COUNSELING AND ADVOCACY PROGRAM
AAA-HICAP-2324-IFB

ADDENDUM ONE

In accordance with Subparagraph 4.1 (County's Right to Amend Invitation for Bids (IFB)) of the Invitation for Bids (IFB), County has the unlimited right to amend the IFB by written addendum. As such, this Addendum is hereby issued for this IFB to address the following elements:

PART I (CHANGES TO THE IFB)

A. IFB Paragraph 1 (Solicitation Information and Minimum Requirements) is deleted in its entirety and replaced as follows:

1. SOLICITATION INFORMATION AND MINIMUM REQUIREMENTS

IFB Release Date	12/13/2022
Request for a Solicitation Requirements Review Due	12/16/2022
Deadline to Register for Mandatory Bidder's Conference	12/16/2022
Mandatory Bidders' Conference	12/19/2022
Written Questions Due	12/19/2022
Questions and Answers Released via Addendum	12/29/2022
Bids Due	01/10/2023
Anticipated Subaward Term	July 1, 2023 – June 20, 2024
Minimum Requirements	Refer to Paragraph 3
IFB Contact	Email:aaarfp@ad.lacounty.gov

B. IFB Subparagraph 7.3 (IFB Timetable) is deleted in its entirety and replaced with the following:

7.3 **IFB Timetable**

The timetable for this IFB is as follows:

EVENT	DATE/TIME
Release of IFB	12/13/2022
Deadline to Submit Request for a Solicitation Requirements Review (Refer to Subparagraph 9 – Protest Process Overview)	12/16/2022
Deadline to Register for Mandatory Bidders' Conference	12/16/2022 5:00 p.m. (P.T.)
Mandatory Bidders' Conference (Refer to Subparagraph 7.5)	12/19/2022 10:00 a.m. (P.T.)
Written Questions Due	12/19/2022 5:00 p.m. (P.T.)
Questions and Answers Released (Subject to change at County's sole discretion)	12/29/2022
Notice of Intent to Submit Bid Due (Refer to Subparagraph 7.9.1)	12/21/2022
Bids Due	01/10/2023 5:00 p.m. (P.T.)

C. IFB Subparagraph 7.7.5.6 (Proof of Licenses (Section E)) is deleted and replaced as follows:

7.7.5.6 **Proof of Licenses, Diploma, and Resume (Section E)**

D. IFB Subparagraph 7.7.5.6.2 is added as follows:

7.7.5.6.2 Bidder must provide a current copy of the resume and diploma from an accredited university in the Social or Behavioral Sciences or a related field for the Project Manager who is reflected in completed Appendix B (Required Forms), Exhibit 10 (Proposed Budget) and Exhibit 11 (Proposed Budget).

PART II (CHANGES TO THE STATEMENT OF WORK)

A. Appendix A (Sample Subaward), Exhibit A (Statement of Work), Subparagraph 2.1 is deleted in its entirety and replaced as follows:

2.1 Services must be provided in Los Angeles County geographic areas, excluding the City of Los Angeles. Prior to modifying or terminating a site, or revising hours of Services at a previously designated location(s), and before commencing such Services at any other location, Subrecipient shall obtain written consent from County, and must comply with Subparagraph 8.1 (Amendments) of this Subaward as applicable.

PART III (ATTACHMENTS TO ADDENDUM ONE)

A. Attachment 1 (AAA-HICAP-2324-IFB Questions and Answers Addendum One) is added as an addendum to this IFB.

B. Exhibit K (Information Security and Privacy Requirements) of Appendix A (Sample Subaward) has been deleted in its entirety and replaced with Exhibit K (Information Security and Privacy Requirements) Revised 12/22/2022. Item 17 (Cyber Liability Insurance) has been updated to reflect the correct cyber liability insurance limits of at least $3,000,000 (3 million) per occurrence.

C. Appendix B (Required Forms), Exhibit 11 (Proposed Budget) is deleted in its entirety and replaced with Appendix B (Required Forms), Exhibit 11 (Proposed Budget), Revised 12/22/2022. Columns (B) Costs and (D) Funding on the Budget Summary Page have been unlocked so that information may be included, if needed. Accordingly, all references made to IFB, Appendix B (Required Forms), Exhibit 11 (Proposed Budget) throughout the IFB and its Appendices will mean the attached Appendix B (Required Forms), Exhibit 11 (Proposed Budget) Revised 12/22/2022.

ATTACHMENT 1
AAA-HICAP-2324 IFB
ADDENDUM ONE
QUESTIONS AND ANSWERS

Pursuant to the IFB Subparagraph 7.4 (Bidders' Questions), this Question and Answer (Q&A) document provides answers to questions received in response to IFB No. AAA-HICAP-2324 IFB. The Q&A have been summarized/edited to capture the essence of the speaker's communication without losing its integrity. Please note that similar questions may have been combined and answered together.

Q1: Please confirm that if an agency did not attend the Mandatory Bidders' Conference, they are not eligible to apply.

Per Subparagraph 7.5.1 of the IFB, all bidders must attend the Mandatory Bidders' Conference, or their bids will be rejected as non-responsive (disqualified) without review and eliminated from further consideration.

Q2: During the Mandatory Bidders' Conference it was stated that there was a 25- page maximum for the entire bid. Please provide the appropriate reference for this in the IFB and what is included and excluded in this page limit (E.G. Exhibits and Attachments).

Subparagraph 7.7 (Bid Format and Review Process) of the IFB does not limit the maximum number of pages.

Q3: Subparagraph B.1 (7.7.5.3) – Is there a minimum or maximum length of the written narrative in pages, words, or characters?

Subparagraph 7.7.5.3.1 (Bidder's Background and Experience (Section B.1)) of the IFB does not reflect a minimum or maximum length for the written narrative.

Q4: For Mandatory Staff, should we list by name in this narrative and provide details about their experience and how they meet the requirements?

The written narrative should be used to list Mandatory Staff (by name) and provide details about their experience and how they meet the requirements in order to meet the Bidder's requirement outlined in Subparagraph 7.7.5.3 (Bidder's Qualifications (Section B)), and Subparagraph 7.7.5.3.1 (Bidder's Background and Experience (Section B.1)) of the IFB.

Q5: "All Mandatory Staff must be listed on Bidder's completed Appendix B (Required Forms)" - Other than this narrative, I do not see a place to list names in the actual forms. Please confirm this is correct.

Bidders should include all mandatory staff *positions* on Bidder's completed Appendix B (Required Forms), Exhibit 10 (Proposed Budget) and Exhibit 11 (Proposed Budget).

Q6: Exhibit 1 (Bidder's Organization Questionnaire) #3 – Is "Proprietor or Managing Partner" the Executive Director?

Non-Profit Organizations should enter "N/A" under "Legal Name of Proprietor or Managing Partner" on Appendix B (Required Forms), Exhibit 1 – Bidder's Organization Questionnaire/Affidavit.

Q7: Exhibit 1 (Bidder's Organization Questionnaire) #13 – Designated Community Focal Points – There are over 50 listed in the Sample Subaward and we currently have over 20. Should we list them all here in addition to in Exhibit 12?

The sites listed on Appendix A (Sample Subaward), Exhibit A (Statement of Work), Attachment 3 (Community Focal Points) is a compilation of designated community focal points within Los Angeles County and is included for reference only.

Per Appendix A (Sample Subaward), Exhibit P (Definitions), Community Focal Point is defined as an agency within the community which has a proven record of providing comprehensive services to older individuals (i.e., multi-purpose senior center).

If your organization has Designated Focal Point(s), your designated focal point information must be identified as such and listed on item 13 of Appendix B (Required Forms) Exhibit 1 – (Bidder's Organization Questionnaire/Affidavit). Bidders should add a separate sheet as needed to reflect all designated focal points.

Focal Points are not required to be listed on Appendix B (Required Forms) Exhibit 12 (Proposed Program Services).

Q8: In Exhibit A (Statement of Work), Subparagraph 2.1 states, "Services must be provided in Los Angeles County geographic areas, including the City of Los Angeles." Since the funding source for this IFB funds the County and City of Los Angeles separately, should we include focal points within the City of Los Angeles in this list?

Paragraph 2 (Addition and/or Deletion of Facilities, Specific Tasks and/or Work Hours, Subparagraph 2.1 of Exhibit A (Statement of Work) of Appendix A (Sample Subaward) of the IFB has been corrected to state, “Services must be provided in Los Angeles County geographic areas, excluding the City of Los Angeles.”

All designated Community Focal Points that are included in Attachment 3 (Community Focal Points List) of Exhibit A (Statement of Work) should be listed.

Q9: Appendix B (Required Forms), Exhibit 6 (Community Business Enterprise Information) – We are a non-profit organization and do not have owners/partners/associate partners. Should this be completed using information about board members?

Non-Profit Organizations should use their Board of Directors’ membership data to complete Appendix B (Required Forms), Exhibit 6 (Community Business Enterprise (CBE) Information).

Q10: Appendix B (Required Forms), Exhibit 9 (Pricing Schedule) – Please define “Estimated Annual Fund (A)” and Bidder’s Annual Fund (B)”.

Estimated Annual Fund (A) is the total anticipated (federal and state) grant funding amount for HICAP and MIPPA Program Services, identified on Appendix B (Required Forms) Exhibit 9 (Pricing Schedule) and in Subparagraph 2.1.6 of Subparagraph 2.1 (Purpose), of the IFB. Bidder’s Annual Fund (B) is the optional Match a Bidder may provide.

Q11: Proof of Insurability – Does the letter need to come from an actual insurance carrier or is a letter from an insurance broker sufficient? Would a quote from within the last year be acceptable documentation?

Written notification (a letter and/or email) from an insurance carrier or broker is sufficient, and a quote from within the last year is acceptable documentation to satisfy the requirement in Subparagraph 7.7.5.5.1 of Subparagraph 7.7.5.5 (Proof of Insurability (Section D)) of the IFB.

Q12: Cyber Insurance Requirement – Current contract requirement is only $250,000. $3,000,000 is a substantial increase. In Exhibit K, #17 of the Sample Subaward, the required coverage is listed as $1,000,000. Please clarify.

The requirement is $3,000,000 as identified in Subparagraph 8.25.8.1 of Subparagraph 8.25 (Insurance Coverage), Appendix A (Sample Subaward).

Exhibit K (Information Security and Privacy Requirements) of Appendix A (Sample Subaward) has been revised to reflect the $3,000,000 requirement. Exhibit K (Information Security and Privacy Requirements) revised 12/22/2022, is Attachment 2 to AAA-HICAP-2324-IFB Addendum One.

Q13: Do you have an anticipated date the selected bidder will be notified of the final determination?

The anticipated notification for the selected bidder will be in February 2023.

Q14: Can you please send/publish a copy of the PowerPoint presentation from the Mandatory Bidders' Conference?

If you are interested in receiving a copy of the PowerPoint presentation from the Mandatory Bidders' Conference, please send an email to aaarfp@ad.lacounty.gov, and we will provide you with a copy.

Q15: Appendix B (Required Forms), Exhibit 8 (Bidder's List of References) and instructions requires a Bidder to provide three (3) references with whom we have a contract, a contract name and number, a contract term, and a contract amount.

For the references, are we required to only list organizations with whom we have a formal contract (such as, for example, the County of Los Angeles and the City of Los Angeles), or is it permissible to list organizations with whom we have worked closely for many years to provide HICAP/MIPPA services, without a formal contract or payment for those services?

Would an agency with whom we have an MOU be appropriate, even if there is no contract name/number/amount?

Or, if we have contracts for the County of Los Angeles, could we then list the County twice, once for one contract and another time for the other contract?

Appendix B (Required Forms), Exhibit 8 (Bidder's List of References) requires a Bidder to provide three (3) references with whom the Bidder has a contract.

For purposes of this IFB, Bidders may include a formal Memorandum of Understanding (MOU) as a reference, provided that the references must be able to substantiate Bidder's experience providing the same or substantially similar scope of Program Services for which Bidder is applying, where such experience has been obtained within the last five (5) years (between 2016-2021).

References must be from separate contracts providing separate services. HICAP has only one (1) Subaward.

Q16: The MIPPA Proposed Budget form for the HICAP IFB, Budget Summary tab will not allow entries into the “10 Months” columns for both Costs (B) and Funding (D).

The corrections have been made Appendix B (Required Forms) Exhibit 11 (Proposed Budget) to allow entries to columns (B) Costs, and (D) Funding of the Budget Summary page, and is reflected in Addendum One of this IFB.

EXHIBIT K
(INFORMATION SECURITY AND PRIVACY REQUIREMENTS)

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 Exhibit K (Information Security and Privacy Requirements) ("Exhibit") set forth County and Subrecipient'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 Subrecipient before the Effective Date of the Subaward and maintained throughout the term of the Subaward.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between County and Subrecipient (the "Subaward") and any other agreements between the parties. However, it is Subrecipient'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 Subaward by Subrecipient, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Subaward, to immediately terminate Subaward. To the extent there are conflicts between this Exhibit and Subaward, this Exhibit shall prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in Subaward, 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 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 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 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 County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

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

Subrecipient'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 Subrecipient 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.

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

Subrecipient's Information Security Program shall:

- Protect the Confidentiality, Integrity, and Availability of County Information in Subrecipient'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 Subrecipient.

b. **Privacy Program.** Subrecipient 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. Subrecipient'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 Subrecipient employees, agents, and volunteers. Subrecipient'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. Subrecipient's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

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

Subrecipient's Privacy Program shall include:

- A Privacy Program framework that identifies and ensures that Subrecipient 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 County, and County shall retain exclusive rights and ownership thereto. County Information shall not be used by Subrecipient for any purpose other than as required under this Subaward, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Subrecipient, or commercially exploited or otherwise used by, or on behalf of, Subrecipient, its officers, directors, employees, or agents. Subrecipient may assert no lien on or right to withhold from County, any County Information it receives from, receives addressed to, or stores on behalf of, County. Notwithstanding the foregoing, Subrecipient 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 Subrecipient, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to 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. Subrecipient specifically consents to County's access to such County Information held, stored, or maintained on any and all devices Subrecipient owns, leases or possesses.

4. SUBRECIPIENT'S USE OF COUNTY INFORMATION

Subrecipient may use County Information only as necessary to carry out its obligations under this Subaward. Subrecipient shall collect, maintain, or use County Information only for the purposes specified in the Subaward 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

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

b. **Disclosure of County Information.** Subrecipient may disclose County Information only as necessary to carry out its obligations under this Subaward, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of County's Contract Manager in consultation with 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, Subrecipient shall notify County's Contract Manager immediately and prior to any such disclosure, to provide 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 Subaward, Subrecipient may encounter County Non-public Information ("NPI") in the course of performing this Subaward, 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. Subrecipient shall not disclose or publish any County NPI and material received or used in performance of this Subaward. This obligation is perpetual.

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

security complaint from an individual regarding County Information, Subrecipient shall notify County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and County will coordinate an appropriate response.

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

7. SUBRECIPIENT EMPLOYEES

Subrecipient shall perform background and security investigation procedures in the manner prescribed in this Section unless the Subaward 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, Subrecipient shall screen and conduct background investigations on all Subrecipient employees and Lower Tier Subrecipients 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 Subrecipient, regardless of whether the member of Subrecipient's staff passes or fails the background investigation. Subrecipient, 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.

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

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

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

8. LOWER TIER SUBRECIPIENTS AND THIRD PARTIES

County acknowledges that in the course of performing its services, Subrecipient may desire or require the use of goods, services, and/or assistance of Lower Tier Subrecipients or other third parties or suppliers. The terms of this Exhibit shall also apply to all Lower Tier Subrecipients and third parties. Subrecipient or third party shall be subject to the following terms and conditions: (i) each Lower Tier Subrecipient 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 Subrecipient 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 Subaward including this Exhibit; and (ii) Subrecipient shall be and remain fully liable for the acts and omissions of each Lower Tier Subrecipient and third party, and fully responsible for the due and proper performance of all Subrecipient obligations under this Subaward.

Subrecipient 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, Subrecipient 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.

Subrecipient will encrypt County Information transmitted on networks outside of Subrecipient'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, Subrecipient 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

Subrecipient shall return or destroy County Information in the manner prescribed in this Section unless the Subaward 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 Subaward for any reason, Subrecipient shall (i) promptly return or destroy, at 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 Subaward; and (iii) deliver or destroy, at 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

Subrecipient, 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 County requests be returned to County, Subrecipient shall provide a written attestation on company letterhead certifying that all documents and materials have been delivered to County. For documents or materials referred to in Subsections (i) and (ii) of this Section that County requests be destroyed, Subrecipient 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 Subaward or at any time upon County's request, Subrecipient shall return all hardware, if any, provided by County to Subrecipient. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by County.

b. **Method of Destruction.** Subrecipient 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 County Information cannot be retrieved. Subrecipient will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and 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's Contract Manager within ten (10) days of termination or expiration of the Subaward or at any time upon County's request. On termination or expiration of this Subaward, County will return or destroy all Subrecipient's Information marked as confidential (excluding items licensed to County hereunder, or that provided to County by Subrecipient hereunder), at County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Subrecipient 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 Subrecipient 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

Subrecipient 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.

Subrecipient 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 Subrecipient 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 Subaward or otherwise expressly approved by the County's Contract Manager or Program 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 Subrecipient and approved by the County's Chief Information Security Officer in writing. The foregoing requirements shall apply to back-up media stored by Subrecipient at off-site facilities.

Subrecipient 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. Subrecipient 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. Subrecipient 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, Subrecipient shall ensure all County Exhibit K (Information Security and Privacy Requirements) Page 11 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, Subrecipient 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:
Ralph Johnson
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:
Scott Enriquez
Departmental Information Security Officer
510 South Vermont Avenue
Los Angeles, CA 90020
(213) 739-7390
senriquez@wdacs.lacounty.gov

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,
   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 County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon County's written request, without charge, unless the Incident was caused by the acts or omissions of County. As Information about the Incident is collected or otherwise becomes available to Subrecipient, and unless prohibited by law, Subrecipient shall provide Information regarding the nature and consequences of the Incident that are reasonably requested by County to allow 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, County, law firms, and and/or law enforcement agencies at the direction of County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with County on any additional disclosures that County is required to make as a result of the Incident.

f. Allow County or its third-party designee at County's election to perform audits and tests of Subrecipient'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 Subaward and Exhibit, Subrecipient 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 Subrecipient's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

Subrecipient 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 County, and therefore, that upon any such breach, 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 Subaward and be grounds for immediate termination of this Subaward in the exclusive discretion of County.

16. AUDIT AND INSPECTION

a. **Self-Audits.** Subrecipient 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 Subrecipient'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 County.

Subrecipient 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. Subrecipient shall provide the audit results and any corrective action documentation to County promptly upon its completion at County's request. With respect to any other report, certification, or audit or test results prepared or received by Subrecipient that contains any County Information, Subrecipient shall promptly provide County with copies of the same upon County's reasonable request, including identification of any failure or exception in Subrecipient's Information systems, products, and services, and the corresponding steps taken by Subrecipient to mitigate such failure or exception. Any reports and related materials provided to County pursuant to this Section shall be provided at no additional charge to County.

b. **County Requested Audits.** At its own expense, County, or an independent third-party auditor commissioned by County, shall have the right to audit Subrecipient'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 County's request Subrecipient shall complete a questionnaire regarding Subrecipient's Information Security and/or program. County shall pay for County requested audit unless the auditor finds that Subrecipient has materially breached this Exhibit, in which case Subrecipient shall bear all costs of the audit; and if the audit reveals material non-compliance with this Exhibit, County may exercise its termination rights underneath the Subaward.

   Such audit shall be conducted during Subrecipient's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Subrecipient's normal business operations. 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 Subrecipient customers such as IP address, server names, etc. Subrecipient shall cooperate with 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 County. Subrecipient agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

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

17. CYBER LIABILITY INSURANCE

Subrecipient shall secure and maintain cyber liability insurance coverage in the manner prescribed in this section unless the Subaward prescribes cyber liability insurance coverage provisions, and those provisions are no less stringent than those described in this section.

Subrecipient shall secure and maintain cyber liability insurance coverage with limits of at least **$3,000,000 (3 million)** per occurrence and in the aggregate during the term of the Subaward, 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 Subaward. Subrecipient 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 Subrecipient'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 Subaward, Subrecipient agrees to indemnify, defend, and hold harmless 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:

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

- Subrecipient's failure to perform or comply with any terms and conditions of this Subaward or related agreements with County; and/or,

- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on Subrecipient's systems or networks (including all costs and expenses incurred by 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, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event Subrecipient fails to provide County with a full and adequate defense, as determined County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from Subrecipient for all such costs and expenses incurred by County in doing so. Subrecipient 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.