PROFESSIONAL SERVICES AGREEMENT

Enterprise Identity and Access Management (IAM) Implementation

BETWEEN

COOK COUNTY GOVERNMENT

COOK COUNTY BUREAU OF TECHNOLOGY

AND

KAPSTONE TECHNOLOGIES LLC D/B/A KAPSTONE, LLC

CONTRACT NO. 2112-18598
PURCHASE ORDER NO. 70000302306

NON-FEDERALLY FUNDED CONTRACT

PROFESSIONAL SERVICES AGREEMENT

TABLE OF CONTENTS

List of Exhibits

AGREEMENT

This Agreement is made and entered into by and between the County of Cook, a public body corporate of the State of Illinois, on behalf of Office of the Chief Procurement Officer hereinafter referred to as "County" and **Kapstone Technologies LLC d/b/a Kapstone, LLC**, doing business as a(an) **Limited Liability Company** of the **State of New Jersey** hereinafter referred to as "Consultant", pursuant to authorization by the Cook County Board of Commissioners on **February 29, 2024**, as evidenced by Board Authorization letter attached hereto as **EXHIBIT "7".**

BACKGROUND

The County of Cook issued a Request for Proposals "RFP" for **Enterprise Identity and Access Management (IAM) Implementation**. ***Proposals were evaluated in accordance with the evaluation criteria published in the RFP. The Consultant was selected based on the proposal submitted and evaluated by the County representatives.***

Consultant represents that it has the professional experience and expertise to provide the necessary services and further warrants that it is ready, willing and able to perform in accordance with the terms and conditions as set forth in this Agreement.

NOW, THEREFORE, the County and Consultant agree as follows:

TERMS AND CONDITIONS

ARTICLE 1) INCORPORATION OF BACKGROUND

The Background information set forth above is incorporated by reference as if fully set forth here.

ARTICLE 2) DEFINITIONS

a) Definitions

The following words and phrases have the following meanings for purposes of this Agreement:

"**Additional Services**" means those services which are within the general scope of Services of this Agreement, but beyond the description of services required under Article 3, and all services reasonably necessary to complete the Additional Services to the standards of performance required by this Agreement. Any Additional Services requested by the Using Agency require the approval of the Chief Procurement Officer in a written amendment to this Agreement before Consultant is obligated to perform those Additional Services and before the County becomes obligated to pay for those Additional Services.

"**Agreement**" means this Professional Services Agreement, including all exhibits attached to it and incorporated in it by reference, and all amendments, modifications or revisions made in accordance with its terms.

"**Chief Procurement Officer**" means the Chief Procurement Officer for the County of Cook and any representative duly authorized in writing to act on his behalf.

"**Services**" means, collectively, the services, duties and responsibilities described in Article 3 of this Agreement and any and all work necessary to complete them or carry them out fully and to the standard of performance required in this Agreement.

"**Subcontractor**" or **"Subconsultant"** means any person or entity with whom Consultant contracts to provide any part of the Services, of any tier, suppliers and materials providers, whether or not in privity with Consultant.

"Using Agency" shall mean the department of agency within Cook County including elected officials.

b) Interpretation

i) The term "**include**" (in all its forms) means "include, without limitation" unless the context clearly states otherwise.

ii) All references in this Agreement to Articles, Sections or Exhibits, unless otherwise expressed or indicated are to the Articles, Sections or Exhibits of this Agreement.

iii) Words importing persons include firms, associations, partnerships, trusts, corporations and other legal entities, including public bodies, as well as natural persons.

iv) Any headings preceding the text of the Articles and Sections of this Agreement, and any tables of contents or marginal notes appended to it are solely for convenience or reference and do not constitute a part of this Agreement, nor do they affect the meaning, construction or effect of this Agreement.

v) Words importing the singular include the plural and vice versa. Words of the masculine gender include the correlative words of the feminine and neuter genders.

vi) All references to a number of days mean calendar days, unless expressly indicated otherwise.

c) Incorporation of Exhibits

The following attached Exhibits are made a part of this Agreement:

Exhibit 1	Scope of Services and Schedule of Compensation
Exhibit 2	SaaS Service Agreement
Exhibit 3	Cook County IT Special Conditions (ITSCs)
Exhibit 4	System Requirements Matrix
Exhibit 5	Minority and Women Owned Business Enterprise Commitment
Exhibit 6	Evidence of Insurance
Exhibit 7	Board Authorization
Exhibit 8	Identification of Subcontractor/Supplier/Subconsultant Form
Exhibit 9	Electronic Payables Program
Exhibit 10	Cook County Travel Policy
Exhibit 11	Economic Disclosure Statement

ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT

a) Scope of Services

This description of Services is intended to be general in nature and is neither a complete description of Consultant's Services nor a limitation on the Services that Consultant is to provide under this Agreement. Consultant must provide the Services in accordance with the standards of performance set forth in Section 3c. The Services that Consultant must provide include, but are not limited to, those described in Exhibit 1, Scope of Services and Time Limits for Performance, which is attached to this Agreement and incorporated by reference as if fully set forth here.

b) Deliverables

In carrying out its Services, Consultant must prepare or provide to the County various Deliverables. "**Deliverables**" include work product, such as written reviews, recommendations, reports and analyses, produced by Consultant for the County.

The County may reject Deliverables that do not include relevant information or data, or do not include all documents or other materials specified in this Agreement or reasonably necessary for the purpose for which the County made this Agreement or for which the County intends to use the Deliverables. If the County determines that Consultant has failed to comply with the foregoing standards, it has 30 days from the discovery to notify Consultant of its failure. If Consultant does not correct the failure, if it is possible to do so, within 15 days after receipt of notice from the County specifying the failure, then the County, by written notice, may treat the failure as a default of this Agreement under Article 9.

Partial or incomplete Deliverables may be accepted for review only when required for a specific and well-defined purpose and when consented to in advance by the County. Such Deliverables will not be considered as satisfying the requirements of this Agreement and partial or incomplete Deliverables in no way relieve Consultant of its commitments under this Agreement.

c) Standard of Performance

Consultant must perform all Services required of it under this Agreement with that degree of skill, care and diligence normally shown by a consultant performing services of a scope and purpose and magnitude comparable with the nature of the Services to be provided under this Agreement. Consultant acknowledges that it is entrusted with or has access to valuable and confidential information and records of the County and with respect to that information, Consultant agrees to be held to the standard of care of a fiduciary.

Consultant must assure that all Services that require the exercise of professional skills or judgment are accomplished by professionals qualified and competent in the applicable discipline and appropriately licensed, if required by law. Consultant must provide copies of any such licenses. Consultant remains responsible for the professional and technical accuracy of all Services or Deliverables furnished, whether by Consultant or its Subconsultants or others on its behalf. All Deliverables must be prepared in a form and content satisfactory to the Using Agency and delivered in a timely manner consistent with the requirements of this Agreement.

If Consultant fails to comply with the foregoing standards, Consultant must perform again, at its own expense, all Services required to be re-performed as a direct or indirect result of that failure.. Any review, approval, acceptance or payment for any of the Services by the County does not relieve Consultant of its responsibility for the professional skill and care and technical accuracy of its Services and Deliverables. This provision in no way limits the County's rights against Consultant either under this Agreement, at law or in equity.

d) Personnel

i) Adequate Staffing

Consultant must, upon receiving a fully executed copy of this Agreement, assign and maintain during the term of this Agreement and any extension of it an adequate staff of competent personnel that is fully equipped, licensed as appropriate, available as needed, qualified and assigned exclusively to perform the Services. Consultant must include among its staff the Key Personnel and positions as identified below. The level of staffing may be revised from time to time by notice in writing from Consultant to the County and with written consent of the County, which consent the County will not withhold unreasonably. If the County fails to object to the revision within 14 days after receiving the notice, then the revision will be considered accepted by the County.

ii) Key Personnel

Consultant must not reassign or replace Key Personnel without the written consent of the County, which consent the County will not unreasonably withhold. "**Key Personnel**" means those job titles and the persons assigned to those positions in accordance with the provisions of this Section 3.d(ii). The Using Agency may at any time in writing notify Consultant that the County will no longer accept performance of Services under this Agreement by one or more Key Personnel listed. Upon that notice Consultant must immediately suspend the services of the key person or persons and must replace him or them in accordance with the terms of this Agreement. A list of Key Personnel is found in Exhibit 1, Scope of Services.

iii) Salaries and Wages

Consultant and Subconsultants must pay all salaries and wages due all employees performing Services under this Agreement unconditionally and at least once a month without deduction or rebate on any account, except only for those payroll deductions that are mandatory by law or are permitted under applicable law and regulations. If in the performance of this Agreement Consultant underpays any such salaries or wages, the Comptroller for the County may withhold, out of payments due to Consultant, an amount sufficient to pay to employees underpaid the difference between the salaries or wages required to be paid under this Agreement and the salaries or wages actually paid these employees for the total number of hours worked. The amounts withheld may be disbursed by the Comptroller for and on account of Consultant to the respective employees to whom they are due. The parties acknowledge that this Section 3.d(iii) is solely for the benefit of the County and that it does not grant any third party beneficiary rights.

e) Minority and Women Owned Business Enterprises Commitment

In the performance of this Agreement, including the procurement and lease of materials or equipment, Consultant must abide by the minority and women's business enterprise commitment requirements of the Cook County Ordinance, (Article IV, Section 34-267 through 272) except to the extent waived by the Compliance Director, which are set forth in **Exhibit 5**. Consultant's completed MBE/WBE Utilization Plan evidencing its compliance with this requirement are a part of this Agreement, in Form 1 of the MBE/WBE Utilization Plan, upon acceptance by the Compliance Director. Consultant must utilize minority and women's business enterprises at the greater of the amounts committed to by the Consultant for this Agreement in accordance with Form 1 of the MBE/WBE Utilization Plan.

f) Insurance

Insurance Requirements

The Consultant, at its cost, shall secure and maintain at all times, unless specified otherwise, until completion of the term of this Contract the insurance specified below.

Nothing contained in these insurance requirements is to be construed as limiting the extent of the Consultant's responsibility for payment of damages resulting from its operations under this Contract.

The Consultant shall require all Subcontractors to provide the insurance required in this Contract, or Consultant may provide the coverages for Subcontractors. All Subcontractors are subject to the same insurance requirements as Consultant unless specified otherwise.

The Cook County Department of Risk Management maintains the right to modify, delete, alter or change these requirements.

Coverages

(a) **Workers Compensation Insurance**

Workers' Compensation shall be in accordance with the laws of the State of Illinois or any other applicable jurisdiction.

The Workers Compensation policy shall also include the following provisions:

Employers' Liability coverage with a limit of
$1,000,000 each Accident
$1,000,000 each Employee
$1,000,000 Policy Limit for Disease

(b) **Commercial General Liability Insurance**

The Commercial General Liability shall be on an occurrence form basis (ISO Form CG 0001 or equivalent) to cover bodily injury, personal injury and property damage.

Each Occurrence	$1,000,000
General Aggregate	$2,000,000
Completed Operations Aggregate	$2,000,000

The General Liability policy shall include the following coverages:

1. All premises and operations;
2. Contractual Liability;
3. Products/Completed Operations;
4. Severability of interest/separation of insureds clause

(c) **Commercial Automobile Liability Insurance**

When any vehicles are used in the performance of this contract, Consultant shall secure Automobile Liability Insurance for bodily injury and property damage arising from the Ownership, maintenance or use of owned, hired and non-owned vehicles with a limit no less than $1,000,000 per accident.

(d) **Professional Liability (Errors & Omissions)**
The Contractor shall secure insurance appropriate to the Contractor's profession covering all claims arising out of the performance or nonperformance of professional services for the County under this Contract. This insurance shall remain in force for the life of the Contractor's obligations under this Contract and shall have a limit of liability of not less than $1,000,000 per claim.

If any such policy is written on a claims-made form:

(1) The retroactive coverage date shall be no later than the effective date of this contract.
(2) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or before this contract effective date, the Contractor must maintain "extended reporting" coverage for a minimum of three (3) year after completion of services.

(e) **Network Security & Privacy Liability (Cyber)**
The Consultant shall secure coverage for first and third-party claims with limits not less than $1,000,000 per occurrence or claim, $1,000,000 aggregate.

If any such policy is written on a claims-made form:

(1) The retroactive coverage date shall be no later than the effective date of this contract.
(2) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or before this contract effective date, the Consultant must maintain "extended reporting" coverage for a minimum of three (3) year after completion of services.

Additional requirements

(a) **Additional Insured**
The required insurance policies, with the exception of Workers Compensation and Errors & Omissions, shall name Cook County, its officials, employees and agents as additional insureds with respect to operations performed on a primary and non-contributory basis. Any insurance or self-insurance maintained by Cook County shall be excess of the Consultant's insurance and shall not contribute with it. The full policy limits and scope of protection shall apply to Cook County as an additional insured even if they exceed the minimum insurance requirements specified herein.

All insurance companies providing coverage shall be licensed or approved by the Department of Insurance, State of Illinois, and shall have a financial rating no lower than (A-) VII as listed in A.M. Best's Key Rating Guide, current edition or interim report. Companies with ratings lower than (A-) VII will be acceptable only upon consent of the Cook County Department of Risk Management. The insurance limits required herein may be satisfied by a combination of primary, umbrella and/or excess liability insurance policies.

(b) **Insurance Notices**

The Consultant shall provide the Office of the Chief Procurement Officer with thirty (30) days advance written notice in the event any required insurance will be cancelled, materially reduced or non-renewed. The Consultant shall secure replacement coverage to comply with the stated insurance requirements and provide new certificates of insurance to the Office of the Chief Procurement Officer.

Prior to the date on which the Consultant commences performance of its part of the work, the Consultant shall furnish to the Office of the Chief Procurement Officer certificates of insurance maintained by Consultant. The receipt of any certificate of insurance does not constitute Contract by the County that the insurance requirements have been fully met or that the insurance policies indicated on the certificate of insurance are in compliance with insurance required above.

In no event shall any failure of the County to receive certificates of insurance required hereof or to demand receipt of such Certificates of Insurance be construed as a waiver of the Consultant's obligations to obtain insurance pursuant to these insurance requirements.

(c) **Waiver of Subrogation Endorsements**

All insurance policies must contain a Waiver of Subrogation Endorsement in favor of Cook County.

g) Indemnification

The Consultant covenants and agrees to indemnify and save harmless the County and its commissioners, officials, employees, agents and representatives, and their respective heirs, successors and assigns, from and against any and all costs, expenses, attorney's fees, losses, damages and liabilities incurred or suffered directly or indirectly from or attributable to any claims arising out of or incident to the performance or nonperformance of the Contract by the Consultant, or the acts or omissions of the officers, agents, employees, Consultants, subconsultants, licensees or invitees of the Consultant. The Consultant expressly understands and agrees that any Performance Bond or insurance protection required of the Consultant, or otherwise provided by the Consultant, shall in no way limit the responsibility to indemnify the County as hereinabove provided.

h) Confidentiality and Ownership of Documents

Consultant acknowledges and agrees that information regarding this Contract is confidential and shall not be disclosed, directly, indirectly or by implication, or be used by Consultant in any way, whether during the term of this Contract or at any time thereafter, except solely as required in the course of Consultant's performance hereunder. Consultant shall comply with the applicable privacy laws and regulations affecting County and will not disclose any of County's records, materials, or other data to any third party. Consultant shall not have the right to compile and distribute statistical analyses and reports utilizing data derived from information or data obtained from County without the prior written approval of County. In the event such approval is given, any such reports published and distributed by Consultant shall be furnished to County without charge.

All documents, data, studies, reports, work product or product created as a result of the performance of the Contract (the "Documents") shall be included in the Deliverables and shall be the property of the County of Cook. It shall be a breach of this Contract for the Consultant to reproduce or use any documents, data, studies, reports, work product or product obtained from the County of Cook or any Documents created hereby, whether such reproduction or use is for Consultant's own purposes or for those of any third party. During the performance of the Contract Consultant shall be responsible of any loss or damage to the Documents while they are in Consultant's possession, and any such loss or damage shall be restored at the expense of the Consultant. The County and its designees shall be afforded full access to the Documents and the work at all times.

i) Patents, Copyrights and Licenses

If applicable, Consultant shall furnish the Chief Procurement Officer with all licenses required for the County to utilize any software, including firmware or middleware, provided by Consultant as part of the Deliverables. Such licenses shall be clearly marked with a reference to the number of this County Contract. Consultant shall also furnish a copy of such licenses to the Chief Procurement Officer. Unless otherwise stated in these Contract documents, such licenses shall be perpetual and shall not limit the number of persons who may utilize the software on behalf of the County.

Consultant agrees to hold harmless and indemnify the County, its officers, agents, employees and affiliates from and defend, as permitted by Illinois law, at its own expense (including reasonable attorneys', accountants' and consultants' fees), any suit or proceeding brought against County based upon a claim that the ownership and/or use of equipment, hardware and software or any part thereof provided to the County or utilized in performing Consultant's services constitutes an infringement of any patent, copyright or license or any other property right.

In the event the use of any equipment, hardware or software or any part thereof is enjoined, Consultant with all reasonable speed and due diligence shall provide or otherwise secure for County, at the Consultant's election, one of the following: the right to continue use of the equipment, hardware or software; an equivalent system having the Specifications as provided in this Contract; or Consultant shall modify the system or its component parts so that they become non-infringing while performing in a substantially similar manner to the original system, meeting the requirements of this Contract.

j) Examination of Records and Audits

The Consultant agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after the final payment under the Contract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices, and records of the Consultant related to the Contract, or to Consultant's compliance with any term, condition or provision thereof.

The Consultant shall be responsible for establishing and maintaining records sufficient to document the costs associated with performance under the terms of this Contract.

The Consultant further agrees that it shall include in all of its subcontracts hereunder a provision to the effect that the Subcontractor agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after final payment under the subcontract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices and records of such Subcontractor involving transactions relating to the subcontract, or to such Subcontractor compliance with any term, condition or provision thereunder or under the Contract.

In the event the Consultant receives payment under the Contract, reimbursement for which is later disallowed by the County, the Consultant shall promptly refund the disallowed amount to the County on request, or at the County's option, the County may credit the amount disallowed from the next payment due or to become due to the Consultant under any contract with the County.

To the extent this Contract pertains to Deliverables which may be reimbursable under the Medicaid or Medicare Programs, Consultant shall retain and make available upon request, for a period of four (4) years after furnishing services pursuant to this Agreement, the contract, books, documents and records which are necessary to certify the nature and extent of the costs of such services if requested by the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives.

If Consultant carries out any of its duties under the Agreement through a subcontract with a related organization involving a value of cost of $10,000.00 or more over a 12 month period, Consultant will cause such subcontract to contain a clause to the effect that, until the expiration of four years after the furnishing of any service pursuant to said subcontract, the related organization will make available upon request of the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives, copies of said subcontract and any books, documents, records and other data of said related organization that are necessary to certify the nature and extent of such costs. This paragraph relating to the retention and production of documents is included because of possible application of Section 1861(v)(1)(I) of the Social Security Act to this Agreement; if this Section should be found to be inapplicable, then this paragraph shall be deemed inoperative and without force and effect.

k) Subcontracting or Assignment of Contract or Contract Funds

Once awarded, this Contract shall not be subcontracted or assigned, in whole or in part, without the advance written approval of the Chief Procurement Officer, which approval shall be granted or withheld at the sole discretion of the Chief Procurement Officer. In no case, however, shall such approval relieve the Consultant from its obligations or change the terms of the Contract. The Consultant shall not transfer or assign any Contract funds or any interest therein due or to become due without the advance written approval of the Chief Procurement

Officer. The unauthorized subcontracting or assignment of the Contract, in whole or in part, or the unauthorized transfer or assignment of any Contract funds, either in whole or in part, or any interest therein, which shall be due or are to become due the Consultant shall have no effect on the County and are null and void.

Prior to the commencement of the Contract, the Consultant shall identify in writing to the Chief Procurement Officer the names of any and all Subcontractors it intends to use in the performance of the Contract by completing the Identification of Subcontractor/Supplier/ Subconsultant Form ("ISF"). The Chief Procurement Officer shall have the right to disapprove any Subcontractor. All Subcontractors shall be subject to the terms of this Contract. Consultant shall incorporate into all subcontracts all of the provisions of the Contract which affect such subcontract. Copies of subcontracts shall be provided to the Chief Procurement Officer upon request.

The Consultant must disclose the name and business address of each Subcontractor, attorney, lobbyist, accountant, consultant and any other person or entity whom the Consultant has retained or expects to retain in connection with the Matter, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant's regular payroll. "Lobbyist" means any person or entity who undertakes to influence any legislation or administrative action on behalf of any person or entity other than: (1) a not-for-profit entity, on an unpaid basis, or (2), himself.

"Lobbyist" also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action. If the Consultant is uncertain whether a disclosure is required under this Section, the Consultant must either ask the County, whether disclosure is required or make the disclosure.

The County reserves the right to prohibit any person from entering any County facility for any reason. All Consultants and Subcontractor of the Consultant shall be accountable to the Chief Procurement Officer or his designee while on any County property and shall abide by all rules and regulations imposed by the County.

l) Professional Social Services

In accordance with 34-146, of the Cook County Procurement Code, all Consultants or providers providing services under a Professional Social Service Contracts or Professional Social Services Agreements, shall submit an annual performance report to the Using Agency, i.e., the agency for whom the Consultant or provider is providing the professional social services, that includes but is not limited to relevant statistics, an empirical analysis where applicable, and a written narrative describing the goals and objectives of the contract or agreement and programmatic outcomes. The annual performance report shall be provided and reported to the Cook County Board of Commissioners by the applicable Using Agency within forty-five days of receipt. Failure of the Consultant or provider to provide an annual performance report will be considered a breach of contract or agreement by the Consultant or provider, and may result in termination of the Contract or agreement.

For purposes of this Section, a Professional Social Service Contract or Professional Social Service Agreement shall mean any contract or agreement with a social service provider, including other governmental agencies, nonprofit organizations, or for profit business enterprises engaged in the field of and providing social services, juvenile justice, mental health treatment, alternative sentencing, offender rehabilitation, recidivism reduction, foster care, substance abuse treatment, domestic violence services, community transitioning services, intervention, or such other similar services which provide mental, social or physical treatment and services to individuals. Said Professional Social Service Contracts or Professional Social Service Agreements do not include CCHHS managed care contracts that CCHHS may enter into with health care providers.

ARTICLE 4) TERM OF PERFORMANCE

a) Term of Performance

This Agreement takes effect when approved by the Cook County Board and its term shall begin on **March 04, 2024** ("**Effective Date**") and continue until **March 03, 2029** or until this Agreement is terminated in accordance with its terms, whichever occurs first.

b) Timeliness of Performance

i) Consultant must provide the Services and Deliverables within the term and within the time limits required under this Agreement, pursuant to the provisions of Section 4.a and **Exhibit 1**. Further, Consultant acknowledges that TIME IS OF THE ESSENCE and that the failure of Consultant to comply with the time limits described in this Section 4.b may result in economic or other losses to the County.

ii) Neither Consultant nor Consultant's agents, employees nor Subcontractors are entitled to any damages from the County, nor is any party entitled to be reimbursed by the County, for damages, charges or other losses or expenses incurred by Consultant by reason of delays or hindrances in the performance of the Services, whether or not caused by the County.

c) Agreement Extension Option

The Chief Procurement Officer may at any time before this Agreement expires elect to renew this Agreement for **two (2) additional, one-year periods** under the same terms and conditions as this original Agreement, except as provided otherwise in this Agreement, by notice in writing to Consultant. After notification by the Chief Procurement Officer, this Agreement must be modified to reflect the time extension in accordance with the provisions of Section 10.c.

ARTICLE 5) COMPENSATION

a) Basis of Payment

The County will pay Consultant according to the Schedule of Compensation in the attached **Exhibit 1** for the successful completion of services.

b) Method of Payment

All invoices submitted by the Consultant shall be in accordance with the cost provisions contained in the Agreement and shall contain a detailed description of the Deliverables, including the quantity of the Deliverables, for which payment is requested. All invoices for services shall include itemized entries indicating the date or time period in which the services were provided, the amount of time spent performing the services, and a detailed description of the services provided during the period of the invoice. All Contracts for services that are procured as Sole Source must also contain a provision requiring the Contractor to submit itemized records indicating the dates that services were provided, a detailed description of the work performed on each such date, and the amount of time spent performing work on each such date. All invoices shall reflect the amounts invoiced by and the amounts paid to the Consultant as of the date of the invoice. Invoices for new charges shall not include "past due" amounts, if any, which amounts must be set forth on a separate invoice. Consultant shall not be entitled to invoice the County for any late fees or other penalties.

In accordance with Section 34-177 of the Cook County Procurement Code, the County shall have a right to set off and subtract from any invoice(s) or Contract price, a sum equal to any fines and penalties, including interest, for any tax or fee delinquency and any debt or obligation owed by the Consultant to the County.

The Consultant acknowledges its duty to ensure the accuracy of all invoices submitted to the County for payment. By submitting the invoices, the Consultant certifies that all itemized entries set forth in the invoices are true and correct. The Consultant acknowledges that by submitting the invoices, it certifies that it has delivered the Deliverables, i.e., the goods, supplies, services or equipment set forth in the Agreement to the Using Agency, or that it has properly performed the services set forth in the Agreement. The invoice must also reflect the dates and amount of time expended in the provision of services under the Agreement. The Consultant acknowledges that any inaccurate statements or negligent or intentional misrepresentations in the invoices shall result in the County exercising all remedies available to it in law and equity including, but not limited to, a delay in payment or non-payment to the Consultant, and reporting the matter to the Cook County Office of the Independent Inspector General.

When a Consultant receives any payment from the County for any supplies, equipment, goods, or services, it has provided to the County pursuant to its Agreement, the Consultant must make payment to its Subcontractors within 15 days after receipt of payment from the County, provided that such Subcontractor has satisfactorily provided the supplies, equipment, goods or services in accordance with the Contract and provided the Consultant with all of the documents and information required of the Consultant. The Consultant may delay or postpone payment to a Subcontractor when the Subcontractor's supplies, equipment, goods, or services do not comply with the requirements of the Contract, the Consultant is acting in good faith, and not in retaliation for a Subcontractor exercising legal or contractual rights.

c) Funding

The source of funds for payments under this Agreement is identified in Exhibit 2, Schedule of Compensation. Payments under this Agreement must not exceed the dollar amount shown in **Exhibit 1** without a written amendment in accordance with Section 10.c.

d) Non-Appropriation

If no funds or insufficient funds are appropriated and budgeted in any fiscal period of the County for payments to be made under this Agreement, then the County will notify Consultant in writing of that occurrence, and this Agreement will terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted. Payments for Services completed to the date of notification will be made to Consultant. No payments will be made or due to Consultant and under this Agreement beyond those amounts appropriated and budgeted by the County to fund payments under this Agreement.

e) Taxes

Federal Excise Tax does not apply to materials purchased by the County by virtue of Exemption Certificate No. 36-75-0038K. Illinois Retailers' Occupation Tax, Use Tax and Municipal Retailers' Occupation Tax do not apply to deliverables, materials or services purchased by the County by virtue of statute. The price or prices quoted herein shall include any and all other federal and/or state, direct and/or indirect taxes which apply to this Contract. The County's State of Illinois Sales Tax Exemption Identification No. is E-9998-2013-07.

f) Price Reduction

If at any time after the contract award, Consultant makes a general price reduction in the price of any of the Deliverables, the equivalent price reduction based on similar quantities and/or considerations shall apply to this Contract for the duration of the Contract period. For purposes of this Section 5.f., Price Reduction, a general price reduction shall include reductions in the effective price charged by Consultant by reason of rebates, financial incentives, discounts, value points or other benefits with respect to the purchase of the Deliverables. Such price reductions shall be effective at the same time and in the same manner as the reduction Consultant makes in the price of the Deliverables to its prospective customers generally.

g) Consultant Credits

To the extent the Consultant gives credits toward future purchases of goods or services, financial incentives, discounts, value points or other benefits based on the purchase of the materials or services provided for under this Contract, such credits belong to the County and not any specific Using Agency. Consultant shall reflect any such credits on its invoices and in the amounts it invoices the County.

ARTICLE 6) DISPUTES

Any dispute arising under the Contract between the County and Consultant shall be decided by the Chief Procurement Officer. The complaining party shall submit a written statement detailing the dispute and specifying the specific relevant Contract provision(s) to the Chief Procurement Officer. Upon request of the Chief Procurement Officer, the party complained against shall respond to the complaint in writing within five days of such request. The Chief Procurement Officer will reduce her decision to writing and mail or otherwise furnish a copy thereof to the Consultant. The decision of the Chief Procurement Officer will be final and binding. Within 60 Business Days after issuance of the final decision, any party to the dispute may appeal the final decision to the Circuit Court of Cook County. Dispute resolution as provided herein shall be a condition precedent to any other action at law or in equity. However, unless a notice is issued by the Chief Procurement Officer indicating that additional time is required to review a dispute, the parties may exercise their contractual remedies, if any, if no decision is made within sixty (60) days following notification to the Chief Procurement Officer of a dispute. No inference shall be drawn from the absence of a decision by the Chief Procurement Officer.
Notwithstanding a dispute, Consultant shall continue to discharge all its obligations, duties and responsibilities set forth in the Contract during any dispute resolution proceeding unless otherwise agreed to by the County in writing.

ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS

The Consultant, Subcontractor, licensees, grantees or persons or businesses who have a County contract, grant, license, or certification of eligibility for County contracts shall abide by all of the applicable provisions of the Office of the Independent Inspector General Ordinance (Section 2-281 et. seq. of the Cook County Code of Ordinances). Failure to cooperate as required may result in monetary and/or other penalties.

The Consultant shall observe and comply with the laws, ordinances, regulations and codes of the Federal, State, County and other local government agencies which may in any manner affect the performance of the Contract including, but not limited to, those County Ordinances set forth in the Certifications attached hereto and incorporated herein. Assurance of compliance with this requirement by the Consultant's employees, agents or Subcontractor shall be the responsibility of the Consultant.

The Consultant shall secure and pay for all federal, state and local licenses, permits and fees required hereunder.

ARTICLE 8) SPECIAL CONDITIONS

a) Warranties and Representations

In connection with signing and carrying out this Agreement, Consultant:

i) warrants that Consultant is appropriately licensed under Illinois law to perform the Services required under this Agreement and will perform no Services for which a professional license is required by law and for which Consultant is not appropriately licensed;

ii) warrants it is financially solvent; it and each of its employees, agents and Subcontractors of any tier are competent to perform the Services required under this Agreement; and Consultant is legally authorized to execute and perform or cause to be performed this Agreement under the terms and conditions stated in this Agreement;

iii) warrants that it will not knowingly use the services of any ineligible consultant or Subcontractor for any purpose in the performance of its Services under this Agreement;

iv) warrants that Consultant and its Subcontractors are not in default at the time this Agreement is signed, and has not been considered by the Chief Procurement Officer to have, within 5 years immediately preceding the date of this Agreement, been found to be in default on any contract awarded by the County;

v) represents that it has carefully examined and analyzed the provisions and requirements of this Agreement; it understands the nature of the Services required; from its own analysis it has satisfied itself as to the nature of all things needed for the performance of this Agreement; this Agreement is feasible of performance in accordance with all of its provisions and requirements, and Consultant warrants it can and will perform, or cause to be performed, the Services in strict accordance with the provisions and requirements of this Agreement;

vi) represents that Consultant and, to the best of its knowledge, its Subcontractors are not in violation of the provisions of the Illinois Criminal Code, 720 ILCS 5/33E as amended; and

vii) acknowledges that any certification, affidavit or acknowledgment made under oath in connection with this Agreement is made under penalty of perjury and, if false, is also cause for termination under Sections 9.a and 9.c.

b) **Ethics**

i) In addition to the foregoing warranties and representations, Consultant warrants:

(1) no officer, agent or employee of the County is employed by Consultant or has a financial interest directly or indirectly in this Agreement or the compensation to be paid under this Agreement except as may be permitted in writing by the Board of Ethics.

(2) no payment, gratuity or offer of employment will be made in connection with this Agreement by or on behalf of any Subcontractors to the prime Consultant or higher tier Subcontractors or anyone associated with them, as an inducement for the award of a subcontract or order.

c) **Joint and Several Liability**

If Consultant, or its successors or assigns, if any, is comprised of more than one individual or other legal entity (or a combination of them), then under this Agreement, each and without limitation every obligation or undertaking in this Agreement to be fulfilled or performed by Consultant is the joint and several obligation or undertaking of each such individual or other legal entity.

d) **Business Documents**

At the request of the County, Consultant must provide copies of its latest articles of incorporation, by-laws and resolutions, or partnership or joint venture agreement, as applicable.

e) **Conflicts of Interest**

i) No member of the governing body of the County or other unit of government and no other officer, employee or agent of the County or other unit of government who exercises any functions or responsibilities in connection with the Services to which this Agreement pertains is permitted to have any personal interest, direct or indirect, in this Agreement. No member of or delegate to the Congress of the United States or the Illinois General Assembly and no Commissioner of the Cook County Board or County employee is allowed to be admitted to any share or part of this Agreement or to any financial benefit to arise from it.

ii) Consultant covenants that it, and to the best of its knowledge, its Subcontractors if any (collectively, "**Consulting Parties**"), presently have no direct or indirect interest and will not acquire any interest, direct or indirect, in any project or contract that would conflict in any manner or degree with the performance of its Services under this Agreement.

iii) Upon the request of the County, Consultant must disclose to the County its past client list and the names of any clients with whom it has an ongoing relationship. Consultant is not permitted to perform any Services for the County on applications or other documents submitted to the County by any of Consultant's past or present clients. If Consultant becomes aware of a conflict, it must immediately stop work on the assignment causing the conflict and notify the County.

iv) Without limiting the foregoing, if the Consulting Parties assist the County in determining the advisability or feasibility of a project or in recommending, researching, preparing, drafting or issuing a request for proposals or bid specifications for a project, the Consulting Parties must not participate, directly or indirectly, as a prime, Subcontractor or joint venturer in that project or in the preparation of a proposal or bid for that project during the term of this Agreement or afterwards. The Consulting Parties may, however, assist the County in reviewing the proposals or bids for the project if none of the Consulting Parties have a relationship with the persons or entities that submitted the proposals or bids for that project.

v) The Consultant further covenants that, in the performance of this Agreement, no person having any conflicting interest will be assigned to perform any Services or have access to any confidential information, as defined in Section 3.h of this Agreement. If the County, by the Chief Procurement Officer in his reasonable judgment, determines that any of Consultant's Services for others conflict with the Services Consultant is to render for the County under this Agreement, Consultant must terminate such other services immediately upon request of the County.

vi) Furthermore, if any federal funds are to be used to compensate or reimburse Consultant under this Agreement, Consultant represents that it is and will remain in compliance with federal restrictions on lobbying set forth in Section 319 of the Department of the Interior and Related Agencies Appropriations Act for Fiscal year 1990, 31 U.S.C. § 1352, and related rules and regulations set forth at 54 Fed. Reg. 52,309 ff. (1989), as amended. If federal funds are to be used, Consultant must execute a Certification Regarding Lobbying, which will be attached as an exhibit and incorporated by reference as if fully set forth here.

f) Non-Liability of Public Officials

Consultant and any assignee or Subcontractor of Consultant must not charge any official, employee or agent of the County personally with any liability or expenses of defense or hold any official, employee or agent of the County personally liable to them under any term or provision of this Agreement or because of the County's execution, attempted execution or any breach of this Agreement.

ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET

a) Events of Default Defined

The following constitute events of default:

i) Any material misrepresentation, whether negligent or willful and whether in the inducement or in the performance, made by Consultant to the County.

ii) Consultant's material failure to perform any of its obligations under this Agreement including the following:

(a) Failure due to a reason or circumstances within Consultant's reasonable control to perform the Services with sufficient personnel and equipment or with sufficient material to ensure the performance of the Services;

(b) Failure to perform the Services in a manner reasonably satisfactory to the Chief Procurement Officer or inability to perform the Services satisfactorily as a result of insolvency, filing for bankruptcy or assignment for the benefit of creditors;

(c) Failure to promptly re-perform within a reasonable time Services that were rejected as erroneous or unsatisfactory;

(d) Discontinuance of the Services for reasons within Consultant's reasonable control; and

(e) Failure to comply with any other material term of this Agreement, including the provisions concerning insurance and nondiscrimination.

iii) Any change in ownership or control of Consultant without the prior written approval of the Chief Procurement Officer, which approval the Chief Procurement Officer will not unreasonably withhold.

iv) Consultant's default under any other agreement it may presently have or may enter into with the County during the life of this Agreement. Consultant acknowledges and agrees that in the event of a default under this Agreement the County may also declare a default under any such other Agreements.

v) Failure to comply with Article 7 in the performance of the Agreement.

vi) Consultant’s repeated or continued violations of County ordinances unrelated to performance under the Agreement that in the opinion of the Chief Procurement Officer indicate a willful or reckless disregard for County laws and regulations.

b) Remedies

The occurrence of any event of default permits the County, at the County's sole option, to declare Consultant in default. If, in the Chief Procurement Officer's sole reasonable discretion, the default is curable, the Chief Procurement Officer will give Consultant an opportunity to cure the default within a certain period of time, which period of time must not exceed 30 days, unless extended by the Chief Procurement Officer. Whether to declare Consultant in default is within the sole discretion of the Chief Procurement Officer and neither that decision nor the factual basis for it is subject to review or challenge under the Disputes provision of this Agreement.

The Chief Procurement Officer will give Consultant written notice of the default, either in the form of a cure notice ("**Cure Notice**"), or, if no opportunity to cure will be granted, a default notice ("**Default Notice**"). If the Chief Procurement Officer gives a Default Notice, he will also indicate any present intent he may have to terminate this Agreement, and the decision to terminate (but not the decision not to terminate) is final and effective upon giving the notice. The Chief Procurement Officer may give a Default Notice if Consultant fails to affect a cure within the cure period given in a Cure Notice. When a Default Notice with intent to terminate is given as provided in this Section 9.b and Article 11, Consultant must discontinue any Services, unless otherwise directed in the notice, and deliver all materials accumulated in the performance of this Agreement, whether completed or in the process, to the County. After giving a Default Notice, the County may invoke any or all of the following remedies:

i) The right to take over and complete the Services, or any part of them, at Consultant's expense and as agent for Consultant, either directly or through others, and bill Consultant for the cost of the Services, and Consultant must pay the difference between the total amount of this bill and the amount the County would have paid Consultant under the terms and conditions of this Agreement for the Services that were assumed by the County as agent for the Consultant under this Section 9.b;

ii) The right to terminate this Agreement as to any or all of the Services yet to be performed effective at a time specified by the County;

iii) The right of specific performance, an injunction or any other appropriate equitable remedy;

iv) The right to money damages;

v) The right to withhold all or any part of Consultant's compensation under this Agreement;

vi) The right to consider Consultant non-responsible in future contracts to be awarded by the County.

If the Chief Procurement Officer considers it to be in the County's best interests, he may elect not to declare default or to terminate this Agreement. The parties acknowledge that this provision is solely for the benefit of the County and that if the County permits Consultant to continue to provide the Services despite one or more events of default, Consultant is in no way relieved of any of its responsibilities, duties or obligations under this Agreement, nor does the County waive or relinquish any of its rights.

The remedies under the terms of this Agreement are not intended to be exclusive of any other remedies provided, but each and every such remedy is cumulative and is in addition to any other remedies, existing now or later, at law, in equity or by statute. No delay or omission to exercise any right or power accruing upon any event of default impairs any such right or power, nor is it a waiver of any event of default nor acquiescence in it, and every such right and power may be exercised from time to time and as often as the County considers expedient.

c) Early Termination

In addition to termination under Sections 9.a and 9.b of this Agreement, the County may terminate this Agreement, or all or any portion of the Services to be performed under it, at any time by a notice in writing from the County to Consultant. The County will give notice to Consultant in accordance with the provisions of Article 11. The effective date of termination will be the date the notice is received by Consultant or the date stated in the notice, whichever is later, which shall not be less than thirty (30) calendar days. If the County elects to terminate this Agreement in full, all Services to be provided under it must cease and all materials that may have been accumulated in performing this Agreement, whether completed or in the process, must be delivered to the County effective 10 days after the date the notice is considered received as provided under Article 11 of this Agreement (if no date is given) or upon the effective date stated in the notice.

After the notice is received, Consultant must restrict its activities, and those of its Subcontractors, to winding down any reports, analyses, or other activities previously begun. No costs incurred after the effective date of the termination are allowed. Payment for any Services actually and satisfactorily performed before the effective date of the termination is on the same basis as set forth in Article 5, but if any compensation is described or provided for on the basis of a period longer than 10 days, then the compensation must be prorated accordingly. No amount of compensation, however, is permitted for anticipated profits on unperformed Services. The County and Consultant must attempt to agree on the amount of compensation to be paid to Consultant, but if not agreed on, the dispute must be settled in accordance with Article 6 of this Agreement. The payment so made to Consultant is in full settlement for all Services satisfactorily performed under this Agreement.

Consultant must include in its contracts with Subcontractors an early termination provision in form and substance equivalent to this early termination provision to prevent claims against the County arising from termination of subcontracts after the early termination. Consultant will not be entitled to make any early termination claims against the County resulting from any Subcontractor's claims against Consultant or the County to the extent inconsistent with this provision.

If the County's election to terminate this Agreement for default under Sections 9.a and 9.b is determined in a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered to be an early termination under this Section 9.c.

d) Suspension

The County may at any time request that Consultant suspend its Services, or any part of them, by giving 15 days prior written notice to Consultant or upon informal oral, or even no notice, in the event of emergency. No costs incurred after the effective date of such suspension are allowed. Consultant must promptly resume its performance of the Services under the same terms and conditions as stated in this Agreement upon written notice by the Chief Procurement Officer and such equitable extension of time as may be mutually agreed upon by the Chief Procurement Officer and Consultant when necessary for continuation or completion of Services. Any additional costs or expenses actually incurred by Consultant as a result of recommencing the Services must be treated in accordance with the compensation provisions under Article 5 of this Agreement.

No suspension of this Agreement is permitted in the aggregate to exceed a period of 45 days within any one year of this Agreement. If the total number of days of suspension exceeds 45 days, Consultant by written notice may treat the suspension as an early termination of this Agreement under Section 9.c.

e) Right to Offset

In connection with performance under this Agreement, the County may offset any excess costs incurred:

i) if the County terminates this Agreement for default or any other reason resulting from Consultant's performance or non-performance;

ii) if the County exercises any of its remedies under Section 9.b of this Agreement; or

iii) if the County has any credits due or has made any overpayments under this Agreement.

The County may offset these excess costs by use of any payment due for Services completed before the County terminated this Agreement or before the County exercised any remedies. If the amount offset is insufficient to cover those excess costs, Consultant is liable for and must promptly remit to the County the balance upon written demand for it. This right to offset is in addition to and not a limitation of any other remedies available to the County.

f) Delays

Consultant agrees that no charges or claims for damages shall be made by Consultant for any delays or hindrances from any cause whatsoever during the progress of any portion of this Contract.

g) Prepaid Fees

In the event this Contract is terminated by either party, for cause or otherwise, and the County has prepaid for any Deliverables, Consultant shall refund to the County, on a prorated basis to the effective date of termination, all amounts prepaid for Deliverables not actually provided as of the effective date of the termination. The refund shall be made within fourteen (14) days of the effective date of termination.

ARTICLE 10) GENERAL CONDITIONS

a) Entire Agreement

i) General

This Agreement, and the exhibits attached to it and incorporated in it, constitute the entire agreement between the parties and no other warranties, inducements, considerations, promises or interpretations are implied or impressed upon this Agreement that are not expressly addressed in this Agreement.

ii) No Collateral Agreements

Consultant acknowledges that, except only for those representations, statements or promises expressly contained in this Agreement and any exhibits attached to it and incorporated by reference in it, no representation, statement or promise, oral or in writing, of any kind whatsoever, by the County, its officials, agents or employees, has induced Consultant to enter into this Agreement or has been relied upon by Consultant, including any with reference to:

(a) the meaning, correctness, suitability or completeness of any provisions or requirements of this Agreement;

(b) the nature of the Services to be performed;

(c) the nature, quantity, quality or volume of any materials, equipment, labor and other facilities needed for the performance of this Agreement;

(d) the general conditions which may in any way affect this Agreement or its performance;

(e) the compensation provisions of this Agreement; or

(f) any other matters, whether similar to or different from those referred to in (a) through (e) immediately above, affecting or having any connection with this Agreement, its negotiation, any discussions of its performance or those employed or connected or concerned with it.

iii) **No Omissions**

Consultant acknowledges that Consultant was given an opportunity to review all documents forming this Agreement before signing this Agreement in order that it might request inclusion in this Agreement of any statement, representation, promise or provision that it desired or on that it wished to place reliance. Consultant did so review those documents, and either every such statement, representation, promise or provision has been included in this Agreement or else, if omitted, Consultant relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Agreement in its entirety without claiming reliance on it or making any other claim on account of its omission.

b) Counterparts

This Agreement is comprised of several identical counterparts, each to be fully signed by the parties and each to be considered an original having identical legal effect.

c) Contract Amendments

The parties may during the term of the Contract make amendments to the Contract but only as provided in this section. Such amendments shall only be made by mutual agreement in writing.

In the case of Contracts not approved by the Board, the Chief Procurement Officer may amend a contract provided that any such amendment does not extend the Contract by more than one (1) year, and further provided that the total cost of all such amendments does not increase the total amount of the Contract beyond $150,000. Such action may only be made with the advance written approval of the Chief Procurement Officer. If the amendment extends the Contract beyond one (1) year or increases the total award amount beyond $150,000, then Board approval will be required.

No Using Agency or employee thereof has authority to make any amendments to this Contract. Any amendments to this Contract made without the express written approval of the Chief Procurement Officer is void and unenforceable.

Consultant is hereby notified that, except for amendments which are made in accordance with this Section10.c. Contract Amendments, no Using Agency or employee thereof has authority to make any amendment to this Contract.

d) Governing Law and Jurisdiction

This Contract shall be governed by and construed under the laws of the State of Illinois. The Consultant irrevocably agrees that, subject to the County's sole and absolute election to the contrary, any action or proceeding in any way, manner or respect arising out of the Contract, or arising from any dispute or controversy arising in connection with or related to the Contract, shall be litigated only in courts within the Circuit Court of Cook County, State of Illinois, and the Consultant consents and submits to the jurisdiction thereof. In accordance with these provisions, Consultant waives any right it may have to transfer or change the venue of any litigation brought against it by the County pursuant to this Contract.

e) Severability

If any provision of this Agreement is held or considered to be or is in fact invalid, illegal, inoperative or unenforceable as applied in any particular case in any jurisdiction or in all cases because it conflicts with any other provision or provisions of this Agreement or of any constitution, statute, ordinance, rule of law or public policy, or for any other reason, those circumstances do not have the effect of rendering the provision in question invalid, illegal, inoperative or unenforceable in any other case or circumstances, or of rendering any other provision or provisions in this Agreement invalid, illegal, inoperative or unenforceable to any extent whatsoever. The invalidity, illegality, inoperativeness or unenforceability of any one or more phrases, sentences, clauses or sections in this Agreement does not affect the remaining portions of this Agreement or any part of it.

f) Assigns

All of the terms and conditions of this Agreement are binding upon and inure to the benefit of the parties and their respective legal representatives, successors and assigns.

g) Cooperation

Consultant must at all times cooperate fully with the County and act in the County's best interests. If this Agreement is terminated for any reason, or if it is to expire on its own terms, Consultant must make every effort to assure an orderly transition to another provider of the Services, if any, orderly demobilization of its own operations in connection with the Services, uninterrupted provision of Services during any transition period and must otherwise comply with the reasonable requests and requirements of the Using Agency in connection with the termination or expiration.

h) Waiver

Nothing in this Agreement authorizes the waiver of a requirement or condition contrary to law or ordinance or that would result in or promote the violation of any federal, state or local law or ordinance.

Whenever under this Agreement the County by a proper authority waives Consultant's performance in any respect or waives a requirement or condition to either the County's or Consultant's performance, the waiver so granted, whether express or implied, only applies to the particular instance and is not a waiver forever or for subsequent instances of the performance, requirement or condition. No such waiver is a modification of this Agreement regardless of the number of times the County may have waived the performance, requirement or condition. Such waivers must be provided to Consultant in writing.

i) Independent Consultant

This Agreement is not intended to and will not constitute, create, give rise to, or otherwise recognize a joint venture, partnership, corporation or other formal business association or organization of any kind between Consultant and the County. The rights and the obligations of the parties are only those expressly set forth in this Agreement. Consultant must perform under this Agreement as an independent Consultant and not as a representative, employee, agent, or partner of the County.

This Agreement is between the County and an independent Consultant and, if Consultant is an individual, nothing provided for under this Agreement constitutes or implies an employer-employee relationship such that:

i) The County will not be liable under or by reason of this Agreement for the payment of any compensation award or damages in connection with the Consultant performing the Services required under this Agreement.

ii) Consultant is not entitled to membership in the County Pension Fund, Group Medical Insurance Program, Group Dental Program, Group Vision Care, Group Life Insurance Program, Deferred Income Program, vacation, sick leave, extended sick leave, or any other benefits ordinarily provided to individuals employed and paid through the regular payrolls of the County.

iv) The County is not required to deduct or withhold any taxes, FICA or other deductions from any compensation provided to the Consultant.

j) Governmental Joint Purchasing Agreement

Pursuant to Section 4 of the Illinois Governmental Joint Purchasing Act (30 ILCS 525) and the Joint Purchase Agreement approved by the Cook County Board of Commissioners (April 9, 1965), other units of government may purchase goods or services under this contract.

In the event that other agencies participate in a joint procurement, the County reserves the right to renegotiate the price to accommodate the larger volume.

k) Comparable Government Procurement

As permitted by the County of Cook, other government entities, if authorized by law, may wish to purchase the goods, supplies, services or equipment under the same terms and conditions contained in this Contract (i.e., comparable government procurement). Each entity wishing to reference this Contract must have prior authorization from the County of Cook and the Consultant. If such participation is authorized, all purchase orders will be issued directly from and shipped directly to the entity requiring the goods, supplies, equipment or services supplies/services. The County shall not be held responsible for any orders placed, deliveries made or payment for the goods, supplies, equipment or services supplies/services ordered by these entities. Each entity reserves the right to determine the amount of goods, supplies, equipment or services it wishes to purchase under this Contract.

l) Force Majeure

Neither Consultant nor County shall be liable for failing to fulfill any obligation under this Contract if such failure is caused by an event beyond such party's reasonable control and which is not caused by such party's fault or negligence. Such events shall be limited to acts of God, acts of war, fires, lightning, floods, epidemics, or riots.

m) Federal Clauses

The following provisions apply to all Contracts which are funded in whole or in part with federal funds including without limitation the following.

1. Interest of Members of or Delegates to the United States Congress
In accordance with 41 U.S.C. § 22, the Contractor agrees that it will not admit any member of or delegate to the United States Congress to any share or part of the Contract or any benefit derived therefrom.

2. False or Fraudulent Statements and Claims
(a) The Contractor recognizes that the requirements of the Program Fraud Civil Remedies Act of 1986, as amended, 49 U.S.C. §§ 3081 et seq and U.S. DOT regulations, "Program Fraud Civil Remedies," 49 C.F.R. Part 31, apply to its actions pertaining to the Contract. Accordingly, by signing the Contract, the Contractor certifies or affirms the truthfulness and accuracy of any statement it has made, it makes, or it may make pertaining to the Contract, including without limitation any invoice for its services. In addition to other penalties that may be applicable, the Contractor also acknowledges that if it makes a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986, as amended, on the Contractor to the extent the Federal Government deems appropriate.

(b) The Contractor also acknowledges that if it makes a false, fictitious, or fraudulent claim, statement, submission, or certification to the County or Federal Government in connection with an urbanized area formula project financed with Federal assistance authorized by 49 U.S.C. § 5307, the Government reserves the right to impose on the Contractor the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 5307(n)(1), to the extent the Federal Government deems appropriate.

3. Federal Interest in Patents

(a) General. If any invention, improvement, or discovery of the Contractor is conceived or first actually reduced to practice in the course of or under the Contract, and that invention, improvement, or discovery is patentable under the laws of the Unites States of America or any foreign country, the Contractor agrees to notify County immediately and provide a detailed report.

(b) Federal Rights. Unless the Federal Government later makes a contrary determination in writing, the rights and responsibilities of the County, Contractor, and the Federal Government pertaining to that invention, improvement, or discovery will be determined in accordance with applicable Federal laws and regulations, including any waiver thereof. Unless the Federal Government later makes a contrary determination in writing, the Contractor agrees that, irrespective of its status or the status of any subcontractor at any tier (e.g., a large business, small business, non profit organization, institution of higher education, individual), the Contractor agrees it will transmit to the Federal Government those rights due the Federal Government in any invention resulting from the contract.

4. Federal Interest in Data and Copyrights

(a) Definition. The term "subject data" used in this section means recorded information, whether or not copyrighted, that is delivered or specified to be delivered under the Contract. Examples include, but are not limited, to: computer software, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog item identifications, and related information. The term "subject data" does not include financial reports, cost analyses, and similar information incidental to Contract administration.

(b) Federal Restrictions. The following restrictions apply to all subject data first produced in the performance of the Contract. Except as provided in the Contract and except for its own internal use, the Contractor may not publish or publicly reproduce subject data in whole or in part, or in any manner or form, nor may the Contractor authorize others to do so, without the written consent of the County and the Federal Government, until such time as the Federal Government may have either released or approved the release of such data to the public.

(c) Federal Rights in Data and Copyrights. In accordance with subparts 34 and 36 of the Common Rule, the County and the Federal Government reserve a royalty free, non exclusive and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for County or Federal Government purposes, the types of subject data described below. Without the copyright owner's consent, the County and Federal Government may not extend their license to other parties.

(1) Any subject data developed under the contract or subagreement financed by a federal Grant Agreement or Cooperative Agreement, whether or not a copyright has been obtained; and

(2) Any rights of copyright which the Contractor purchases ownership with Federal assistance.

(d) Special Federal Rights for Planning Research and Development Projects. When the Federal Government provides financial assistance for a planning, research, development, or demonstration project, its general intention is to increase public knowledge, rather than limit the benefits of the project to participants in the project. Therefore, unless the Federal Government determines otherwise, the Contractor on a planning, research, development, or demonstration project agrees that, in addition to the rights in data and copyrights set forth above, the County or Federal Government may make available to any third party either a license in the copyright to the subject data or a copy of the subject data. If the project is not completed for any reason whatsoever, all data developed under the project will become subject data and will be delivered as the County or Federal Government may direct. This subsection, however, does not apply to adaptions of automatic data processing equipment or previously existing software programs for the County's use whose costs are financed with Federal transportation funds for capital projects.

(e) Hold Harmless. Unless prohibited by state law, upon request by the County or the Federal Government, the Contractor agrees to indemnify, save, and hold harmless the County and the Federal Government and their officers, agents, and employees acting within the scope of their official duties against any liability, including costs and expenses, resulting from any willful or intentional violation by the Contractor of proprietary rights, copyrights, or right of privacy, arising out of the publication, translation, reproduction, delivery, use, or disposition of any data furnished under the Contract. The Contractor will not be required to indemnify the County or Federal Government for any such liability arising out of the wrongful acts of employees or agents of the County or Federal Government.

(f) Restrictions on Access to Patent Rights. Nothing contained in this section on rights in data will imply a license to the County or Federal Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the County or Federal Government under any patent.

(g) Application on Materials Incorporated into Project. The requirements of Subsections 2, 3, and 4 of this Section do not apply to material furnished by the County and incorporated into the work.

5. Records and Audits

Contractor will deliver or cause to be delivered all documents (including but not limited to all Deliverables and supporting data, records, graphs, charts and notes) prepared by or for the County under the terms of this Agreement to the County promptly in accordance with the time limits prescribed in this Contract, and if no time limit is specified, then upon reasonable demand therefor or upon termination or completion of the Services hereunder. In the event of the failure by the Contractor to make such delivery, then and in that event, the Contractor will pay to County reasonable damages the County may sustain by reason thereof.

The County and the Federal Government will have the right to audit all payments made to the Contractor under this Agreement. Any payments to the Contractor which exceed the amount to which the Contractor is entitled under the terms of this Agreement will be subject to set off.

The Contractor will keep and retain records relating to this Agreement and will make such records available to representatives of the County and the Federal Government, including without limitation the sponsoring federal agency, other participating agencies, and the Comptroller General of the United States, at reasonable times during the performance of this Agreement and for at least five years after termination of this Agreement for purposes of audit, inspection, copying, transcribing and abstracting.

No provision in this Agreement granting the County or the Federal Government a right of access to records is intended to impair, limit or affect any right of access to such records which the County or the Federal Government would have had in the absence of such provisions.

6. Environmental Requirements

The Contractor recognizes that many Federal and state laws imposing environmental and resource conservation requirements may apply to the Contract. Some, but not all, of the major Federal Laws that may affect the Contract include: the National Environmental Policy Act of 1969, as amended, 42 U.S.C. §§ 4321 et seq.; the Clean Air Act, as amended, 42 U.S.C. §§ 7401 et seq. and scattered sections of 29 U.S.C.; the Clean Water Act, as amended, scattered sections of 33 U.S.C. and 12 U.S.C.; the Resource Conservation and Recovery Act, as amended, 42 U.S.C. §§ 6901 et seq.; and the Comprehensive Environmental Response, Compensation, and Liability Act, as amended, 42 U.S.C. §§ 9601 et seq. The Contractor also recognizes that U.S. EPA, U.S. DOT and other agencies of the Federal Government have issued and are expected in the future to issue regulations, guidelines, standards, orders, directives, or other requirements that may affect the Contract. Thus, the Contractor agrees to adhere to, and impose on its subcontractors, any such Federal requirements as the Federal Government may now or in the future promulgate. Listed below are requirements of particular concern.

The Contractor acknowledges that this list does not constitute the Contractor's entire obligation to meet all Federal environmental and resource conservation requirements. The Contractor will include these provisions in all subcontracts.

(a) Environmental Protection. The Contractor agrees to comply with the applicable requirements of the National Environmental Policy Act of 1969, as amended, 42 U.S.C. §§ 4321 et seq. in accordance with Executive Order No. 12898, "Federal Actions to Address Environmental Justice in Minority Populations and Low Income Populations," 59 Fed. Reg. 7629, Feb. 16, 1994; U.S. DOT statutory requirements on environmental matters at 49 U.S.C. § 5324(b); Council on Environmental Quality regulations on compliance with the National Environmental Policy Act of 1969, as amended, 40 C.F.R. Part 1500 et seq.; and U.S. DOT regulations, "Environmental Impact and Related Procedures," 23 C.F.R. Part 771 and 49 C.F.R. Part 622.

(b) Air Quality. The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. §§ 7401 et seq. Specifically, the Contractor agrees to comply with applicable requirements of U.S. EPA regulations, "Conformity to State of Federal Implementation Plans of Transportation Plans, Programs, and Projects Developed, Funded or Approved Under Title 23 U.S.C. or the Federal Transit Act," 40 C.F.R. Part 51, Subpart T; and "Determining Conformity of

Federal Actions to State or Federal Implementation Plans," 40 C.F.R. Part 93. The Contractor further agrees to report and require each subcontractor at any tier to report any violation of these requirements resulting from any Contract implementation activity to the County and the appropriate U.S. EPA Regional Office.

(c) Clean Water. The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. §§ 1251 et seq. The Contractor further agrees to report and require each subcontractor at any tier to report any violation of these requirements resulting from any Contract implementation activity to the County and the appropriate U.S. EPA Regional Office.

(d) List of Violating Facilities. The Contractor agrees that any facility to be used in the performance of the Contract or to benefit from the Contract will not be listed on the U.S. EPA List of Violating Facilities ("List"), and the Contractor will promptly notify the County if the Contractor receives any communication from the U.S. EPA that such a facility is under consideration for inclusion on the List.

(e) Preference for Recycled Products. To the extent practicable and economically feasible and to the extent that it does not reduce or impair the quality of the work, the Contractor agrees to use recycled products in performance of the Contract pursuant to U.S. Environment Protection Agency (U.S. EPA) guidelines at 40 C.F.R. Parts 247 253, which implement section 6002 of the Resource Conservation and Recovery Act, as amended, 42 U.S.C. § 6962.

7. No Exclusionary or Discriminatory Specifications

Apart from inconsistent requirements imposed by Federal statute or regulations, the Contractor agrees that it will comply with the requirements of 49 U.S.C. § 5323(h)(2) by refraining from using any Federal assistance to support subcontracts procured using exclusionary or discriminatory specifications.

8. No Federal Government Obligations to Third Parties

The Contractor agrees that, absent the Federal Government's express written consent, the Federal Government will not be subject to any obligations or liabilities to any contractor or any other person not a party to the Grant Agreement or Cooperative Agreement between the County and the Federal Government which is a source of funds for this Contract. Notwithstanding any concurrence provided by the Federal Government in or approval of any solicitation, agreement, or contract, the Federal Government continues to have no obligations or liabilities to any party, including the Contractor.

9. Allowable Costs

Notwithstanding any compensation provision to the contrary, the Contractor's compensation under this Contract will be limited to those amounts which are allowable and allocable to the Contract in accordance with OMB Circular A 87 and the regulations in 49 C.F.R. Part 18. To the extent that an audit reveals that the Contractor has received payment in excess of such amounts, the County may offset such excess payments against any future payments due to the Contractor and, if no future payments are due or if future payments are less than such excess, the Contractor will promptly refund the amount of the excess payments to the County.

10. Trade Restrictions

Contractor certifies that neither it nor any Subcontractor:

(a) is owned or controlled by one or more citizens of a foreign country included in the list of countries that discriminate against U.S. firms published by the Office of the United States Trade Representative (USTR);

(b) has knowingly entered into any contract or subcontract with a person that is a citizen or national of a foreign country on said list, nor is owned or controlled directly or indirectly by one or more citizens or nationals of a foreign country on said list;

(c) will procure, subcontract for, or recommend any product that is produced in a foreign country on said list.

Unless the restrictions of this clause are waived by the Secretary of Transportation in accordance with 49 CFR 30.17, no Notice to Proceed will be issued to an entity who is unable to certify to the above. If Contractor knowingly procures or subcontracts for the supply of any product or service of a foreign country on said list for use on the project, the USDOT may direct, through the County, cancellation of the Contract at no cost to the Government.

Further, Contractor agrees that it will incorporate this provision for certification without modification in each subcontract. Contractor may rely on the certification of a prospective Subcontractor unless it has knowledge that the certification is erroneous. Contractor will provide immediate written notice to the County if it learns that its certification or that of a Subcontractor was erroneous when submitted or has become erroneous by reason of changed circumstances. Each Subcontractor must agree to provide written notice to Contractor if at any time it learns that its certification was erroneous by reason of changed circumstances. Nothing contained in the foregoing will be construed to require establishment of a system of records in order to render, in good faith, the certification required by this provision.

The knowledge and information of the Contractor is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

This certification concerns a matter within the jurisdiction of an agency of the United States of America and the making of a false, fictitious, or fraudulent certification may render the maker subject to prosecution under Title 18, United States Code, Section 100.

11. Contract Work Hours and Safety Standards Act

If applicable according to their terms, the Contractor agrees to comply and assures compliance with sections 102 and 107 of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. §§ 327 through 333, and implementing U.S. DOL regulations, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction (also Labor Standards Provisions Applicable to Nonconstruction Contracts Subject to the Contract Work Hours and Safety Standards Act)," 29 C.F.R. Part 5; and U.S. DOL regulations, "Safety and Health Regulations for Construction," 29 C.F.R. Part 1926. In addition to other requirements that may apply:

(a) In accordance with section of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. §§ 327 through 332, the Contractor agrees and assures that, for the Contract, the wages of every mechanic and laborer will be computed on the basis of a standard work week of 40 hours, and that each worker will be compensated for work exceeding the standard work week at a rate of not less than 1.5 times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The Contractor agrees that determinations pertaining to these requirements will be made in accordance with applicable U.S. DOL regulations, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction (also Labor Standards Provisions Applicable to Nonconstruction Contracts Subject to the Contract Work Hours and Safety Standards Act)," 29 C.F.R. Part 5.

(b) In accordance with section 107 of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. § 333, the contractor agrees and assures that no laborer or mechanic working on a construction contract will be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous to his or her health and safety, as determined in accordance with U.S. DOL regulations, "Safety and Health Regulations for Construction," 29 C.F.R. Part 1926.

12. Copyright Ownership

Consultant and the County intend that, to the extent permitted by law, the Deliverables to be produced by Consultant at the County's instance and expense pursuant to this Agreement are conclusively deemed "works made for hire" within the meaning and purview of Section 101 of the United States Copyright Act, 17 U.S.C. §101 et seq. (the "Copyright Act"), and that the County will be the copyright owner of the Deliverables and of all aspects, elements and components of them in which copyright can subsist.

To the extent that any Deliverable does not qualify as a "work made for hire," Consultant irrevocably grants, conveys, bargains, sells, assigns, transfers and delivers to the County, its successors and assigns, all right, title and interest in and to the copyrights and all U.S. and foreign copyright registrations, copyright applications and copyright renewals for them, and other intangible, intellectual property embodied in or pertaining to the Deliverables prepared for the County under this Agreement, free and clear of any liens, claims or other encumbrances, to the fullest extent permitted by law. Consultant will execute all documents and perform all acts that the County may reasonably request in order to assist the County in perfecting its rights in and to the copyrights relating to the Deliverables, at the sole expense of the County.

Consultant warrants to County, its successors and assigns, that on the date of transfer Consultant is the lawful owner of good and marketable title in and to the copyrights for the Deliverables and has the legal rights to fully assign them. Consultant further warrants that it has not assigned any copyrights nor granted any licenses, exclusive or nonexclusive, to any other party, and that it is not a party to any other agreements or subject to any other restrictions with respect to the Deliverables. Consultant warrants and represents that the Deliverables are complete and comprehensive, and the Deliverables are a work of original authorship.

13. Visual Rights Act Waiver

The Consultant/Contractor waives any and all rights that may be granted or conferred under Section 106A and Section 113 of the United States Copyright Act, (17 U.S.C. § 101 et seq.) (the "Copyright Act") in any work of visual art that may be provided pursuant to this Agreement. Also, the Consultant/Contractor represents and warrants that the

Consultant/Contractor has obtained a waiver of Section 106A and Section 113 of the Copyright Act as necessary from any employees and subcontractors, if any.

14. Equal Employment Opportunity

During the performance of this contract, the contractor agrees as follows:

(1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

(4) The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared

ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: Provided, That if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

15. Copeland "Anti-Kickback" Act (40 U.S.C. 3145))
All contracts and subgrants in excess of $2000 for construction or repair awarded by recipients and subrecipients shall include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient shall be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled. The recipient shall report all suspected or reported violations to the Federal awarding agency.

16. Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708)
Where applicable, all contracts awarded by recipients in excess of $100,000 that involve the employment of mechanics or laborers shall include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR part 5). Under 40 U.S.C. 3702 of the Act, each contractor shall be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than 1 ½ times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provides that no laborer or mechanic shall be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

17. Rights to Inventions Made Under a Contract or Agreement
Contracts or agreements for the performance of experimental, developmental, or research work shall provide for the rights of the Federal Government and the recipient in any resulting invention in accordance with 37 CFR part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

18. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended
Contracts and subgrants of amounts in excess of $150,000 shall contain a provision that requires the recipient to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.). Violations shall be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

19. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)
Contractors who apply or bid for an award of $100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal

appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient.

20. Debarment and Suspension (E.O.s 12549 and 12689)
No contract shall be made to parties listed on the General Services Administration's List of Parties Excluded from Federal Procurement or Nonprocurement Programs in accordance with E.O.s 12549 and 12689, "Debarment and Suspension." This list contains the names of parties debarred, suspended, or otherwise excluded by agencies, and contractors declared ineligible under statutory or regulatory authority other than E.O. 12549. Contractors with awards that exceed the small purchase threshold shall provide the required certification regarding its exclusion status and that of its principal employees.

ARTICLE 11) NOTICES

All notices required pursuant to this Contract shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if hand delivered or if deposited in the United States mail, postage prepaid, registered or certified, return receipt requested. Notice as provided herein does not waive service of summons or process.

If to the County: Cook County Bureau of Technology
161 N. Clark Street, Suite 500
Chicago, Illinois 60601
Attention: Department Director

and

Cook County Office of the Chief Procurement Officer
161 N. Clark Street, Suite 2300
Chicago, Illinois 60601
(Include County Contract Number 2112-18598 on all notices)

If to Consultant: Kapstone Technologies LLC
370 Campus Drive, #108
Somerset, NJ 08873
Attention: Harish Jangada

Changes in these addresses must be in writing and delivered in accordance with the provisions of this Article 11. Notices delivered by mail are considered received three days after mailing in accordance with this Article 11. Notices delivered personally are considered effective upon receipt. Refusal to accept delivery has the same effect as receipt.

ARTICLE 12) AUTHORITY

Execution of this Agreement by Consultant is authorized by a resolution of its Board of Directors, if a corporation, or similar governing document, and the signature(s) of each person signing on behalf of Consultant have been made with complete and full authority to commit Consultant to all terms and conditions of this Agreement, including each and every representation, certification and warranty contained in it, including the representations, certifications and warranties collectively incorporated by reference in it.

EXHIBIT 1

Scope of Services and Schedule of Compensation

COOK COUNTY GOVERNMENT

Statement of Work (SOW) for Enterprise Identity and Access Management Implementation
Contract No: 2112-18598
Contract Term: March 04th, 2024 – March 03rd , 2029
Vendor: Kapstone Technologies LLC
Date: October 9th, 2023
Version: V1.2

TABLE OF CONTENTS

1. Executive Summary.

This Executive Summary section is intended as an overview of the Cook County Government ("CCG" or "County") objectives for the project, scope and timeline for the Enterprise Identity and Access Management ("IAM") Implementation project.

This Statement of Work (SOW) is intended to document the scope, schedule, roles, responsibilities, tasks and assumptions for the implementation of the IAM at the County. This SOW will be the governing project document, outlining project milestones as mutually agreed to by both parties.

1.1. Definitions.

For purposes of this SOW, Appendix A list capitalized terms used and not defined herein shall have the respective meanings ascribed to them.

1.2. Background.

The CCG is in the process of implementing an enterprise-wide identity and access management (c) system. The CCG needs to implement a full suite of Identity and Access Management (IAM) capabilities to support integration to agency systems.

To build an enterprise IAM system, CCG has partnered with **Kapstone,** a qualified Systems Integrator with extensive experience in implementing large-scale enterprise IAM projects.

CCG seeks Kapstone to design and implement the solutions with County owned software and suggest gaps in software or services as needed by working with County's agencies and vendors to create best practices for policy governance functions. Among others, Proposer design/implemented solution shall include, but not limited to

a) Systems health checks
b) Assure higher system availability SLAs.
c) Implement the central solution using modular approach for feature/function reusability.
d) Design, implement, and monitor the solution to isolate the breaches for very minimal impact on the overall system.
e) Establish and manage the process controls for preventive and pro-active monitoring of the central platform.
f) Establish the frameworks to collect audit and usage data.

The IAM implementation will help CCG to provide a central streamlined platform for all staff and service providers (employees, contractors, vendors, suppliers, other government agencies). The implementation will provide Role-based and rule-based access management services, that will improve end-user experience and reduce risk within the enterprise. Other benefits of the project include:

- Highly reliable solution on a hybrid-cloud environment
- Standardized integration between the IAM suite and IT resources to improve access lead times and accuracy.
- Real-time automation of identity lifecycle management and access controls

- Off load development efforts from application teams
- Reduce costs by providing a centralized enforcement platform.
- Modernize CCG IT environment strategically.
- Increase compliant and secured industry posture.
- Satisfy business needs, industry, and government regulations requirements.
- Common automated processes across the lines of business

1.3. Project Objective.

Kapstone understands that CCG's business objective for the Enterprise Identity and Access Management (IAM) implementation and support program is to improve agency and bureau collaboration on common enterprise-wide processes such as employee onboarding, offboarding, and securing privileged user access to County resources. This will be achieved by deploying a unified, flexible process across the agencies, and documenting the agency-specific process variations and compliances. County is also seeking to achieve a standards-based platform for agencies' internal applications to provide secure access to its employees, contractors, and citizens. This transformational project will help the County to achieve operational excellence to support regulatory requirements for CJIS, PII and FIPS.

The high-level technical objective for the program is to build a highly fault-tolerant, scalable, open standards-driven IAM platform that can meet various current and future requirements and migrate current IAM functions to the new platform. Once built, this IAM platform is expected to provide the following goals and objectives:

a) Identify, document, and implement Agency specific processes for user on-boarding and off-boarding.
b) Develop a unified process, enforcing Agency specific policies using workflows and governance.
c) Establish a centralized policy management tool/framework from design time to runtime.
d) Implement privileged user access management framework to achieve Agency specific statutory legal compliances.
e) Self-service portal for Citizen password management
f) Establish a repeatable checklist-based process for Application on-boarding and off-boarding to make use of the central Identity and Access Management toolset.
g) Citizen profile management, one central application for citizen user registration, profile management, communication preferences and self-service password management
h) Unified Citizen Dashboard for County applications – One set of credentials, County applications identify the citizen. Each application provides needed access to the citizen.
i) Integrate with Security framework tools for end-to-end tracking of the user/device actions.
j) Develop identity analytics for issue patterns, reports, and notifications.
k) Integration with Social identity frameworks using standards (Google email ID, Facebook ID etc.)

Overall, the Enterprise IAM implementation and support program is expected to improve the efficiency and security of County's IAM processes, while also reducing costs.

1.4. Project Scope.

Kapstone will build an Enterprise IAM Platform using Oracle Identity and Access Management suite of products. The project will be implemented in three phases as listed below.

- **Phase 1** will be focused on planning, requirement analysis and platform design for the IAM platform.
- **Phase 2** will be focused on building the foundational IAM platform with core services.
- **Phase 3** will be focused on application on-boarding activities and continuous integrations.

Phase 1 (Planning, requirement analysis and platform design for the IAM platform)

Conduct Requirement workshops and create solution design for the following use cases:

- Application Authentication and Authorizations: Authentication, web SSO, coarse-grained authorization for web applications deployed on-premises or in the cloud.
- Identity Federation: Support Cross-Internet-domain authentication and delegated authorization supporting industry standards such as SAML, OAuth, and OpenID Connect. Social logon using social network identities.
- Adaptive Access and Risk Analysis: Setup multi-factor authentication and the heuristic fraud detection service.
- Standards Based Integration: Adopt open standards such as OAuth, OpenID Connect, SAML, and FIDO2 where possible for heterogeneous environment coexistence. Leverage REST APIs for federation management, multi data center, OAuth, password management, multi-factor authentication, OTP, password policy, and session management.
- Application on-boarding: IAM product's self-service UI for configuring application instances, entitlements, workflows, approvers, risk etc. for defining access requests and reconciliation for Administrators. It will allow administrators to add descriptions for Application Instances, Entitlements and Roles with description. Additionally, the solution will have functionality for compliance and certifications. Application owners and access approvers will be able to review and approve meta data information of application before it is available for access to end-users.
- Application Retirement: Admins will be able to remove all access for end-users. Also, they will be able to remove all artifacts related to application from OIM. This includes features such as workflows, access related components, reconciliation, provisioning, certification etc.
- Access Reconciliation: Kapstone will migrate CCG's existing reconciliation process for trusted and target applications. Kapstone will implement access reconciliation processes for connected and disconnected applications.
- Application Metadata maintenance: Admins and application owners will have capability to modify attributes of applications and entitlement. These attributes include approver details, risk classification, access related components and compliance rules for active application.
- Access Request, Approval and Provisioning: Users will be able to submit access requests for themselves or on behalf of other users for access to an entitlement or a role with justification as mandatory field. The entitlements and Roles will be descriptive, so that end-users can easily identify them. All access requests before submission will be validated for any type of pre-

requisite such as training or SODs or background checks etc. Submission of duplicate access requests will be handled appropriately. Additionally, access will be revoked based on future end-date or user status or emergency revocation by manager or application owners.

- Access Request workflow: Access requests will be configurable to allow up to 3 levels of approvals. The solution will be open to include additional approval levels as needed – for those requests needing SOD/Training, the requests are sent to SOD/Training approval groups as 4th level. The managers will get notifications with actionable email for approvals of request workflow. The access requests requiring training will connect to CCG learning systems to validate status of training status and training curriculum before account can be provisioned to target system. Access requests submitted by managers will be auto approved. Approvals based on time or for reassignment will be assigned to groups. Provisioning tasks for disconnected tasks will send appropriate email notifications.
- Provisioning and de-provisioning: Provisioning or de-provisioning will be triggered based on request approval, certification results, transfer, or termination event to different targets such as AD Groups, PeopleSoft, Oracle DB, IDCS, IBM RACF and OpenLDAP. Disconnected applications will support provisioning and de-provisioning tasks to Groups with required details for provisioning instructions in request. Additionally, disconnected applications will allow single step provisioning where required. In case of a need to revoke a user's application accounts and entitlement access immediately, the design will have provision for such emergency revocation by passing all approvals from the application owners.
- RBAC Framework: Role management framework will be in place to migrate, govern, and retire roles. Role governance and retire role will trigger approval workflow and impact analysis where applicable. Provisioning of role to end users will be open both policy/rule-based provisioning as well as based on request being raised and approved. Role certification framework will include certification of roles to their policy definition as well as review and certification entitlements contained within them. Kapstone will use its custom utility to discover roles and track changes to role definition that can be leveraged in Role definition certification. In addition, Kapstone collaborates with CCG IAM SME to implement role retirement process including making role as non-requestable, remove/hide from catalog items, and develop role event handler for advanced role management. Request workflows will allow submission of access request involving multiple Roles and it will be based on Access Policies with Rule based provisioning and de-provisioning.
- Role Life Cycle Management: It will allow CCG to migrate existing roles and role membership to 12c OIM and retire roles based on business requirement. Role requests can leverage the same request and approval framework available for Access Requests and Certification. Role owners will be able to perform comprehensive role certification.
- Access Certification: There will be capability to initiate access certification manually or automatically on a pre-defined schedule for application instances and entitlements based on users, application, entitlement, roles, role definition, certifiable and compliance type. The certification process will be scheduled for service accounts and human accounts, under a manager. Bulk approvals will require justification for any decision inclusive of approval, rejection or conditional approval. Conditional approvals and approvals require last comments to be pre-filled for provisioning or certification. The rejected account/entitlement access will result in de-

provisioning. An un-certification can only be reassigned to a different owner. There will be capability to generate user certification campaigns. Initiation and completion of each certification cycle will be logged for traceability. In the event of any failure in between certification cycles, the solution will log the point of failure and notify the admins, and, in which case, reiteration of the certification will resume from the point of failure.

- Transfer User: Kapstone will migrate existing transfer user process to IAM platform. Kapstone will migrate compliance configuration for transfer user process to IAM platform.
- Contractor Renewal: Kapstone will migrate the existing contractor renewal process to IAM platform as is. Kapstone will migrate compliance configuration for contractor renewal process to EIAM. Kapstone will configure contractor renewal use cases.
- Periodic Entitlement Review: Certification will be annually triggered for application attributes and approval groups for application owners.
- Compliance Checks and Tracking: Scheduled validation of background checks, training status and SOD violations and take appropriate action of removal of access for non-compliance except for service accounts and process ids. Ensure that PII data is tracked, and appropriate measures are taken for handling sensitive data during migration of data. There needs to be traceability of initiation and completion of scheduled tasks and a notification will be sent out for failed tasks. Scheduled tasks related to certification of all entities such as users/service ids/application accounts/entitlements, provisioning/de-provisioning, and open tasks for disconnected applications. There will be appropriate actions available for failed tasks. A change management process to ensure that application and their metadata meets compliance requirements. Track all rouge accounts are handled appropriately as per defined process. Track refresh of any custom views or tables.
- SOD Life Cycle Management: It will allow to define toxic combinations of entitlements, which no one user will possess. It will ensure that fraud cannot be committed without collusion by multiple people. It will allow CCG to implement preventive/detective policy enforcement. Preventive enforcement will trigger a SOD violation at access request initiation and appropriate preventive action will be taken. Detective enforcement will detect any SOD violations by generating reports and remediate violations after the fact. While enforcing SOD policies, OIM will handle SOD use case specific to non-human account / service accounts.
- Process / Service Account Management: Service accounts will be requested, provisioned, and managed the same as regular accounts. During its lifecycle, OIM will allow to change or move service account owner to different user or group. If the owner of a service account changes, OIM will send appropriate alerts.
- ITSM: Integrate ServiceNow with OIM for service account lifecycle management.
- IAM Governance for In-flight and On-Going Changes: Any in-flight and ongoing changes need to be handled appropriately during implementation.
- SOA Workflow: Migrate SOA workflow to 12c. Handle implicit manager approval.
- Reports: Setup enterprise grade reporting platform to meet regulatory and operational reporting requirements
- Privilege Account Management: CyberArk to be implemented as the PAM (Privilege Account Management) solution

- Application and User Onboarding: Identifying all source and target applications and planning their onboarding.
- Data Migration: Data migration requirements and validation.

Phase 2 (focused on building the foundational IAM platform with core services)

- Build 12c OIM, OUD, OAM, OAA, OARM (OIAM) infrastructure with high availability following Oracle's best practices and documentation.
- Setup OIAM on containers using Containerization platform like Tanzu, OpenShift, OKE, EKS….
- Enable TLS1.2+ protocol for secure communication in 12c OIAM for WebLogic, Database, and Identity Connector server.
- Optionally, Migrate 11g OIAM data from database to 12c OIAM, inclusive of application domains, authentication and authorization modules, user, entitlement, roles, application instances, custom code, auditing data, certification data and additional workflow configurations.
- Migrate configurations and workflows from 11g OIM to 12c OIM. Some of the configurations can be exported using deployment manager, the ones that cannot be exported will be migrated manually.
- If there are customizations added in authentication plug-ins, provisioning, reconciliation, certification, scheduler etc. for meeting business requirements. These customizations must be migrated to 12c OIAM, even if there is code change required, business functionality will remain same.
- Develop a unified process for user access management, enforcing Agency specific policies using workflows and governance.
- Establish a centralized policy management tool/framework, where possible, from design time to runtime for Identity Governance policies, request approval policies, access control policies, Identity Administrations policies, Authentication and Authorization policies.
- Setup integrations with IDPs like Azure AD and ADFS
- Established Zero-Trust framework. Established multi-factor authentication framework. Setup authentication orchestrations plug-ins that can be extendible to handle IP based restrictions, bring your own authentication, bring your own MFA, intranet access, VPN access and external facing application access.
- Setup Citizen / external user on-boarding interfaces (API framework, approval workflows, on-boarding processes, strong authentication enrollment, account verification / validation / proofing)
- Setup federation services, OAUTH, OIDC, SAML 2.0, Windows native authentications integration services on OIAM platform.
- Setup core common IAM services for authentication, authorization, application on-boarding, workflows, access controls, governance, compliance, and audit reporting. Document the process and on-board up to 5 applications (to be identified during discovery phase) onto centralized unified platform for authentication and authorization requirements.
- Integrate with Active directory and up to 8 other agency applications (to be identified during discovery phase). Integrate with HR authoritative sources.

- Conduct performance tuning of OIAM 12c and Database for OIAM.
- Implement archival and purging available with 12c OIAM according to CCG's policies for data growth utilizing OOTB utilities provided by Oracle for archival, purging and compression of data.
- Provide documentation guide for implementation, user guide for end-users.
- Create a disaster recovery plan for RTO and RPO of 48 hours meeting the SLA for Disaster recovery. OIAM will be deployed in Active-Passive mode with data synchronized between Production and DR environment using Data Guard or Active Data Guard. Or OIM will be deployed in Active-Active mode with both application layers pointing to active database. Setup OAM using multi-data center architecture in active-active mode. During the design phase, Kapstone will provide inputs on DR installation.
- Conduct in-person or virtual / online class to train end-users and CCG's OIAM project team with usage of new system.
- The Kapstone will assist CCG team in setting it up for 12 OIAM artifacts into antifactory and will be integrated with automation pipeline tools like Jenkins. Additionally, these need to be version controlled.
- Log management will be consolidated and log data shall be sent in a secure manner to the log management tool that CCG uses within the enterprise. Log data shall be sent in a format compatible with the CCG log management tool.
- CCG is planning to implement PAM solution. Based on the decision by CCG and availability of PAM solution, OIM will be integrated with PAM using SCIM connector or LDAP bridge approach.
- Solution will cover role management; role governance and role certification and custom utility can be used to create roles in bulk into OIM.
- SOD rules will be reviewed and based on the findings by Kapstone. If required, a recommendation will be proposed for better optimizing existing SOD design in EIAM.
- Automation tools, Scripts and strategy will be provided for functional testing of critical processes.
- Any critical issues raised during the Cyber Security testing on production deployed version, Kapstone will analyze and provide necessary support.

Phase 3 (focused on application on-boarding activities and continuous integrations)

- Application Onboarding
  - Integrate with and up to 8 other agency applications (to be identified during discovery phase).
- Privileged Access Management
  - Build and Configure Privileged Access Management Solution in up to 3 environments.
  - Integrate PAM with OIM and OAM
  - Integrate OAM with up to 5 applications for password management.
- Operational Support

  Create and configure reports and analytics to assist in operations support and

  i. Perform proactive/preventive monitoring and to determine the solution critical path components of such activities as listed below:
     - Perform Root Cause Analysis, Developing custom tools/scripts where applicable.
     - Resolve Tickets
     - Monitor Systems availability
     - Set up notifications for System access breach.
     - Conduct DR cycles

- Manage and support Cloud environment.

ii. Set up Alerts for

- User activity, where user performs activities occasionally or ad hoc basis.
- For large query executions; Large import or export of files, data etc.
- For high volume (by transaction count or transaction volume) activity by single user or single device or single location

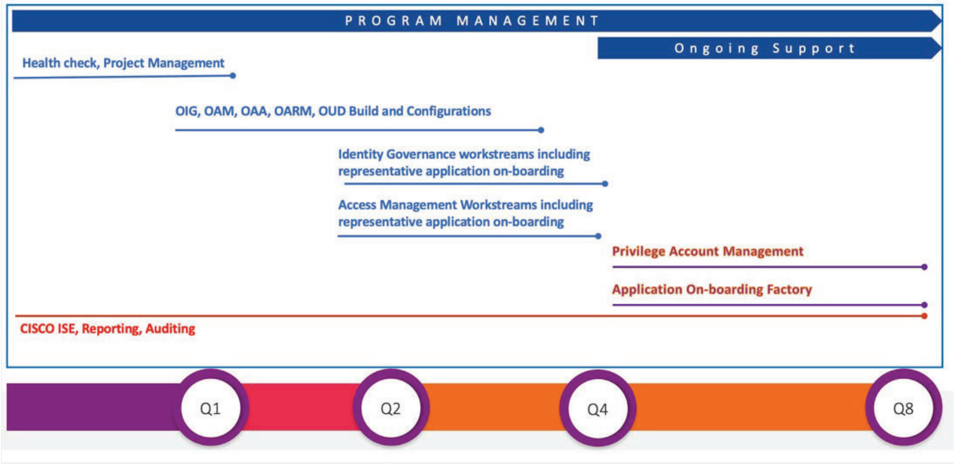
1.5. Software Installation and Configuration

The County will procure or will ensure licenses for all software applications listed in this section. The County will procure licenses for all necessary IAM platforms. Kapstone will install and configure the Oracle IAM and PAM, vendor yet to be decided, technology components listed below:

- Oracle HTTP Server
- Oracle Linux
- Oracle WebLogic Suite
- Oracle Identity and Access Management Suite (OIM, OAM, OUD, OAA, OARM)
- Oracle WebLogic Server Management
- Oracle OCI
- CloudNuro.ai – SaaS Management Platform
- SOA Suite
- SOA Management Pack
- Oracle IAM Containers
- PAM solution
- BI publisher
- MS Azure
- CyberArk PAM

1.6. Period of Performance.

The services under this SOW will commence on 5th March 2024 (the start date is contingent on approval of the County Board) and be complete five-Years from the Start Date (the "SOW/Project Completion Date"). Below diagrams depicts eight quarters (Q – quarter as three months) engagement plan, with first four quarters will be focused on building the IAM environment and next four quarters will be used for application on-boarding and refining IAM processes.


PROGRAM MANAGEMENT
Ongoing Support
Health check, Project Management
OIG, OAM, OAA, OARM, OUD Build and Configurations
Identity Governance workstreams including representative application on-boarding
Access Management Workstreams including representative application on-boarding
Privilege Account Management
Application On-boarding Factory
CISCO ISE, Reporting, Auditing
Q1
Q2
Q4
Q8

The planning, implementation of IAM platform and pilot application / agency on-boarding is expected to be completed in twenty-four months from the start date. The year-two to year-five will be focused on optimizing run and operate processes, maintenance, and support.

2. Scope of Service.

The scope of services associated with the implementation of IAM are listed in this section.

2.1. Project Execution

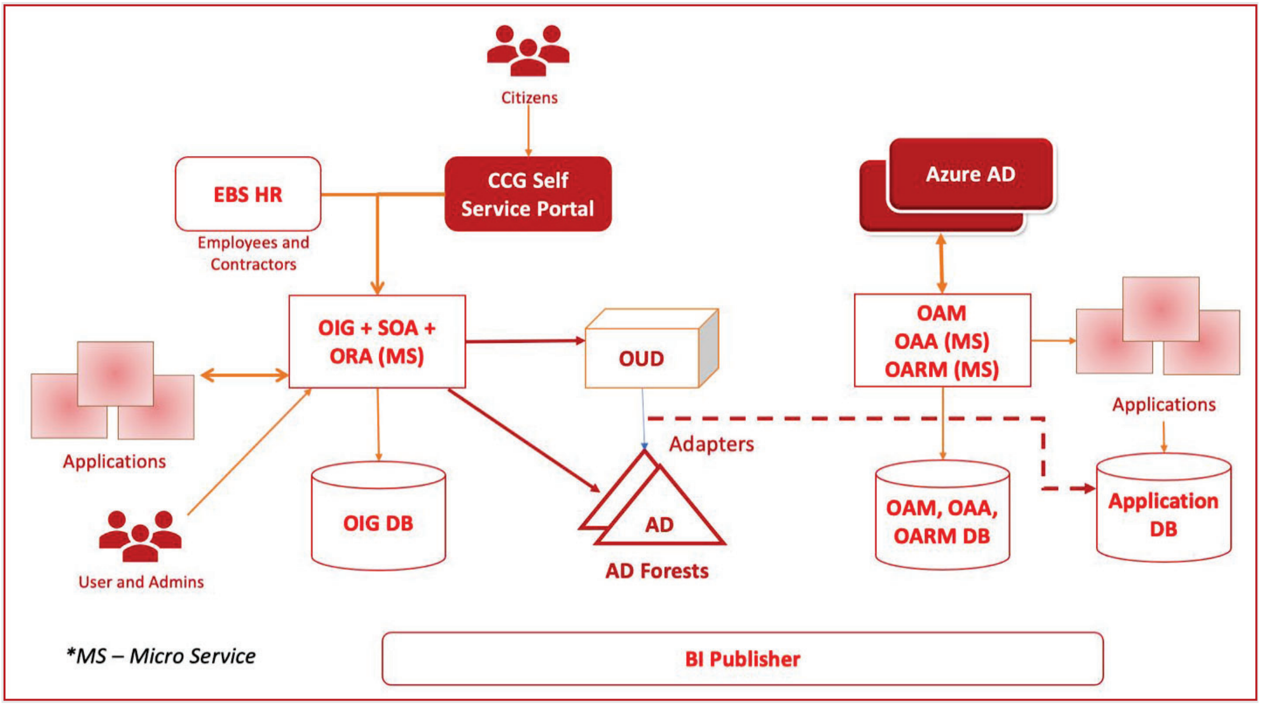
Kapstone will follow the County's BOT centric approach in collaboration with IT, PMO and other stakeholders (other agencies) for implementing Identity and Access Management platform for the County, which includes the following services:

- **Program and Project Management:** Kapstone will establish the necessary charter, governance, tools, and resources to create and maintain a Project Office including coordination and collaboration with County project management personnel.
- **Discovery, Project Preparation:** Kapstone will be involved in reviewing existing documentation and working with key project members to validate scope, planning, constraints, project organization, previously developed requirements, analysis, and artifacts.
- **Requirements Analysis and Design: This i**ncludes reviewing functional and technical requirements, including information security controls, business process documentation in order to develop County specific requirements and system design.
- **System Configuration, Set-up, Development:** Includes installation of system environment(s) configuring, developing business and technical requirements, services, components and the like.
- **Data Migration:** The includes migration of data, resources in the new environment, including setting up a process for a secured data migration, in non-production and production environment.
- **Testing:** Includes creation of test strategy, plan and scripts, test execution and validation of the design requirements including security component and monitoring.
- **Training and Knowledge Transfer:** Includes the development of training materials, conducting Train-The-Trainer training for users and technical staff and knowledge transfer to the County staff.
- **Go-Live:** Includes production deployment of the solution, services and components, etc.
- **Post-Production Production Support:** Provide extended post-production support for six weeks, after the production deployment.
- **Managed Support Service:** Provide managed support service to Cook County for deployed IAM environment.

Kapstone will project plan with CCG's program lifecycle processes like integration, scope, schedule, resources, risks, and communication, and will update the project plan which will be aligned with the County's schedule and staff availability.

2.2. Solution Architecture, Integration, Migration and Deployment

In the proposed system flow diagram shown below, Oracle Identity and Access Management Solution (OIAM) 12c PS4 and CyberArk (as PAM solution) to address the CCG'S IAM requirements. Additional design consideration details are included in **Appendix C.**



The CCG's Oracle E-business Suite will be used as an authoritative source for the employees, contractors and CCG's self-service portal will be used as the interface for external users. CCG self-service portal will be updated to leverage OIG API interface to provide self-service and password management capabilities.

- Microsoft IAM (Legacy MIIM, ADFS and Microsoft's strategic IAM platform Azure AD) will co-exist with Oracle IAM solution. Wherever applicable, MIIM services will be migrated to Azure AD Connect and Oracle Identity Governance solution for provisioning or account life cycle management solution. All SSO, MFA and Conditional services will be configured on Microsoft Azure AD and Oracle IAM solution. Microsoft Azure AD will serve internal users (employees and contractors) and will be configured as IdP.

- OUD directory will be the authentication and authorization store for the applications. OUD will have native accounts and as well as DB & AD adapters will be configured for the delegated authentication or for password validations. Web Applications will be integrated into the new IAM platform and OAM will provide the authentication and authorization services for the new on-boarded applications. OAM will support and enable federation services framework that facilitates trust and interoperability between agencies for cross agency user authentication. All Web applications will be integrated into the Oracle access management (OAM, OAA and OARM) to provide the authentication and authorization, multi-factor, adaptive/ risk-based authentication and federation services. OAA and OARM (New versions of OAAM) will be used to provide multifactor authentication services for the new applications as needed.
- OIG will provision users into OUD and Employees reconciled from PeopleSoft into AD and OUD. OIG will be used for user life cycle management, access reviews, request management & approval, segregation od duties management and orphan account managements.

- ORA will be used for Role Mining and the output of the role mining exercise will be used to configure birthright access to various applications.
- BI Publisher will be used for Identity administration and governance and access management reporting purposes and will pull the data from OIG, OAM, OAA, OARM databases.
- For PAM, CyberArk to manage privileged accounts in Database, Windows and Linux / Unix by limiting access to them to authorized users and by protecting passwords and distributing them to authorized individuals on as needed basis.. The Kapstone will perform privilege account management discovery and provide recommendations to the CCG team to evaluate and select the product.
- ITSM tickets will be generated via emails from OIG for manual provisioning of devices (mobile, phone, etc).

  The IAM components described in the high-level solutions are mapped to CCG's requirements as shown in table below.

Component	Requirement	Provided Functionality
Oracle Access Manager (OAM)	Single Sign On	Provides user authentication and Single Sign On across all protected applications. User is not being prompted for credentials while traversing through protected applications as long as a user's session remains valid. OAM will provide SAML or OIDC authentication to SaaS applications. Webgate can be configured on the proxy servers to provide http header-based integration for Single Sign-on.
Oracle Unified Directory (OUD)	Directory Services	Directory Service as provided by OUD will centrally store user data. The authoritative source of this data will be Oracle EBS and CCG Citizen self-service interface .
Oracle Advanced authentication (OAA)	Multi Factor Authentication	MFA feature of OAA will provide a second level of authentication utilizing factors such as email, SMS or Oracle Mobile Authenticator
Oracle Adaptive Risk Management (OARM)	Adaptive Authentication	OARM will provide configurable method for selecting the appropriate authentication factors depending on a user's risk profile and behavior adapting the type of authentication to the situation, as part of an ongoing process
Oracle Identity Governance (OIG or OIM)	User Identity Management	OIG provides automated ability to provision and de-provision users across target systems. This will include processes like user onboarding, access changes based on role change, user offboarding etc.
Oracle Identity Governance	User Self Service	OIG provides the workflow-based capabilities for User Self Service functions like Password Change/Reset, Profile update etc.

Oracle Identity Governance	Identity Governance	OIG will provide the ability to perform security audits to review user access entitlements across the entire system. It also provides the ability to address user privilege creep, stale accounts, orphan accounts, and shared accounts.
Oracle Access Manager	Identity Federation	Provides user authentication and Single Sign On across domains and organization utilizing industry standard protocols such as SAML and OAuth.
BI Publisher	Audit and Reporting	BI Publisher will provide reporting capabilities. With capabilities to pull and join data from multiple sources it is a very powerful tool to monitor user access, account statuses, etc.
CloudNuro.ai	Cloud Services Management and Support	Governance and managed services for Cloud platform.
CyberArk	Privileged Access Management	CyberArk will provide functionality of storing, checking in and out passwords. Passwords will be stored in CyberArk and will remain unknown to anyone within the organization. Upon request, subject to approvals, passwords will be checked out by CyberArk and provided to authorized users. Upon completion of the task users will check the passwords back in and CyberArk will change them, removing elevated access. CyberArk will protect Linux, Windows and database accounts.

2.2.1. Solution Design and Implementation Services

IAM design and implementation services includes the below key services:

Identity Administration and Governance

- **Application Onboarding**: Kapstone will configure OIM 12c provided connectors for integration with different type of target systems. With 12c OIM application on-boarding has been simplified for Admins and it allows cloning as well as developing templates for onboarding similar type of applications. Application onboarding will be used, if available for the target application, to **create templates** for connected as well as disconnected applications. Kapstone will leverage configurations options to add approver details as well as risk classifications for Applications as well as Entitlements. Various delegated roles for different functionalities, application admin role will be configured to allow application owners or IAM admins to create applications with required mappings.
- **Application offboarding/Retirement**: - Kapstone will define the agency specific process to offboard an application to ensure that it is not available for requesting, provisioning, reconciliation or review certification check. The retired application will not be removed from OIM environment; it will be available only to OIM Admins for Audit purposes after it has been retired.

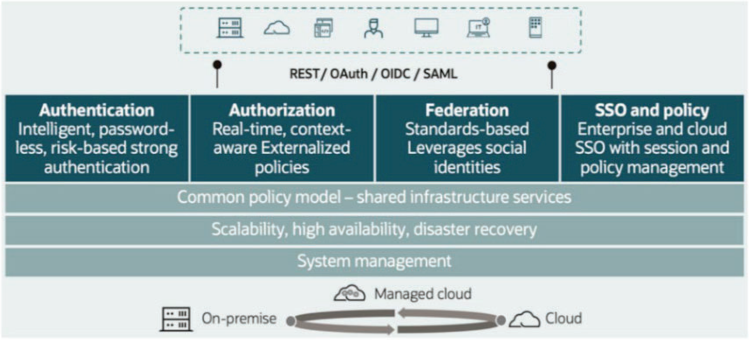
- **Application Metadata Maintenance:** Kapstone will define different attributes of metadata such as risk level, approver users/roles, certifier users/roles and fulfilment roles/users. Additionally, Business rules will be defined for rule-based access in OIM.
- **Access Request, Approval & Provisioning**: OIM will be configured to allow users to request access for self and others with justification and to revoke request for a Role and an Entitlement with multi-level approval workflows for fulfilment of request. The centralized core workflow will be configured for access request and provisioning. These workflows will be configured to integrate with agency specific processes via hooks, manual processes or external asynchronous calls. Access Request process will be integrated with ITSM (Cherwell) solution, if APIs will be available.
- **Access Request Workflow**: - OIM leverages SOA composites for workflows and are highly customizable. Composites will be configured as per business requirements. It will be used for notification scenarios such as request creations, reminders emails, request completion, expiry actions and can be configured as per business needs. Additionally, proxies will be assigned for a duration in case an approver is unavailable. Lightweight workflow, including web-based composure, is in Oracle's product roadmap and that will be used in future and remove the dependencies on SOA component. New lightweight workflow solution will bring significant performance benefits to the overall OIM solution.
- **Provisioning and De-provisioning**: Business rules will be configured for automated provisioning/de-provisioning based on Roles, which will automatically assign/revoke access. Additionally, access will be disabled / revoked as a part of certification process. In case a user doesn't have an account in the requested application, then account will be provisioned, and the entitlement will be assigned to that user. If a user already has an account in target system, then entitlement will directly be assigned to the user after approval of request.
- **Access Certification**: Kapstone will configure user access review as per the requirements. OIM has built in functionality to review and certify user access, with a user-friendly interface called as identity certification, it is available to managers, authorized users, and compliance administrators. Authorized administrators have option to create and configure certification campaigns, on a scheduled or ad-hoc basis, using wizards. The interface for certifying the user access provides a simplified view to certifiers, making overall certification process easy for approving the access or rejecting it. When a violation is detected, a rejected flow is invoked causing OIM to initiate a process that enables administrators to correct the violation. It will be configured to directly deprovision the account from the target system or application, while maintaining a comprehensive trail of the actions taken. This is also known as closed-loop remediation. OIM supports comprehensive list of certifications, based on criteria such as user, managers, role owners, application owners, and entitlement owners.
- **Transfer User**: OIM provides administration based on role-based access controls. Roles make it easier to assign access levels to users and to audit those assignments on an ongoing basis. Rather than assigning access levels to users directly, access levels

are assigned to a role. Roles are assigned to users, and a user's access level is determined by the roles assigned to that user. Roles will be designed using provisioning policies so that a user access privileges can be modified as user transfers.

- **Contractor Renewal**: Certification campaign will be configured based on user criteria thus creating separate campaign for Employees and Contractors. Additionally, these campaigns will be scheduled as per business needs.
- **Compliance Checks and Trainings**: Compliance reports will be generated on a schedule basis and actions will be taken based on the reports. Audit and exception reports will be configured and used for reviews or certifications to ensure users have appropriate access and are in compliance. Additionally, business requirements will be met with customization option available with OIM.
- **Reports**: Audit data and data related modifications are stored in different tables of OIM database schema and can be fed to any reporting tool that supports reading data from Oracle database to generate the reports. Query is executed in real-time and provides most current data in reports. OIM by default provides BIP publisher reports for standard reporting requirements. Custom reports will be generated for business requirements as historical data is stored in OIM database till it is purged based on retention policy.

<u>Access Management (Zero Trust, Authentication, MFA and Authorization) and Directory Services</u>

The following diagram shows the Oracle Access management core components.


REST / OAuth / OIDC / SAML
Authentication
Intelligent, password-less, risk-based strong authentication
Authorization
Real-time, context-aware Externalized policies
Federation
Standards-based Leverages social identities
SSO and policy
Enterprise and cloud SSO with session and policy management
Common policy model – shared infrastructure services
Scalability, high availability, disaster recovery
System management
Managed cloud
On-premise
Cloud

- **Single Sign-On**
  - Kapstone will enable SAML and OpenID protocol on the OAM in addition to request header-based authentication option. OAM supports both SAML and OpenID Connect standards to provide SSO capabilities. It acts as a hub to provide SSO between cross platform applications that support industry standard protocols SAML and OpenID Connect.
  - Kapstone will set up webgates or web agents to integrate with on-premises applications such as Oracle E-Business as these applications do not yet support SAML or OpenID Connect and rely on HTTP header authentication.
- **Multi-Factor Authentication**
  - Kapstone will setup Azure AD MFA options configure Multi-Factor Authentication (MFA) options on OAM. MFA is a method of authentication that

requires the use of more than one factor to verify a user's identity. With MFA enabled in Oracle Advanced Authentication, when a user signs into an application, they are prompted for their username and password, which is the first factor – something that they know. The user is then required to provide a second type of verification. This is called 2-Step Verification. The two factors work together to add an additional layer of security by using either additional information or a second device to verify the user's identity and complete the login process. MFA may include any two factors (Password, OTP via SMS, OTP via email, Mobile Authenticator)

  - Kapstone will configure adaptive authentication and or passwordless authentication using OAA and OARM. Adaptive Authentication is an advanced feature that provides strong authentication capabilities for enterprise users, based on their behavior within OAA and OARM, and across multiple heterogeneous on-premises applications and cloud services.
  - Kapstone will configure OARM's risk profile feature. The Adaptive Authentication feature can analyze a user's risk profile within OARM on their historical behavior, such as too many unsuccessful login attempts, too many unsuccessful MFA attempts, and real-time device context like logins from unknown devices, access from unknown locations, blacklisted IP addresses, and so on.

- User Authentication Store
  - Kapstone will integrate OUD and AD with OAM for user store requirements. Oracle Unified Directory will be populated by users from the authoritative source. Adapters for Databases will be configured to perform password validation. The users will be loaded into OUD via ldif or using OIG/OIM.
- Virtual Directory
  - OUD will be configured to provide virtualization capabilities.
- **Identity Federation:** OAM will be configured for Cross-Internet-domain authentication and delegated authorization supporting industry standards such as SAML, OAuth, and OpenID Connect.
- **Adaptive Access and Risk Analysis**: Using multifactor authentication and the heuristic fraud detection service, the Oracle Mobile Authenticator (OMA) provides soft-token TOTP solutions with one-touch notification services as well as Passwordless access with OMA push notifications.
- **Oracle Advanced Authentication (OAA):** FIDO2 and YubiKey modern Passwordless factors featured will be enabled to enhance MFA capabilities. If needed Oracle RADIUS Agent (ORA) will be configured to help protect Oracle databases, VPN, and SSH sessions with modern MFA user experience.
- **Password Management:** OIG and OAM will be configured to support multiple password policies, enabling varied levels of password-based complexity protection for users belonging to different groups. The reset and forgot password capability can be supported with second factor authentication methods and out-of-band TOTP.

- **Multi Data Center Lifecycle Simplification**: OAM will be configured using MDC option. New REST based APIs will be used to configure MDC and it will significantly reduce the number of configuration steps performed in the MDC environment. OAuth Artifacts (such as Identity Domains, Clients, Resources, etc. created in one data center are visible and seamlessly synchronized across other data centers.
- **OAuth Consent Management**: Consent Management will be enabled for each of the OAuth Identity Domains or all the OAuth Identity Domains in OAM.
- **OAuth Just-In-Time (JIT) Provisioning**: JIT user provisioning will be enabled a user identity to be provisioned dynamically when the user tries to login for the first time using any social identity providers, If needed. User account creation is done directly, without the need to provision users in the system, in advance. JIT feature can be used to implement progressive profiling for citizen services.
- **Standards Based Integration:** Kapstone will integrate application using standard based integration where possible. Adoption of open standards such as OAuth, OpenID Connect, SAML, and FIDO2 allows for heterogeneous environment coexistence.
- **Webgate:** The 12c version of Webgate will be used for header variable-based application integration requirements.
- **Integration:** Develop integrations for user federation and authentication, including the following:
  a) Oracle Identity Federation
  b) Multi-factor authentication
  c) Integration with SMS Services
  d) Integrations with OAuth providers (Google, MS)

2.2.2. Application integration and onboarding

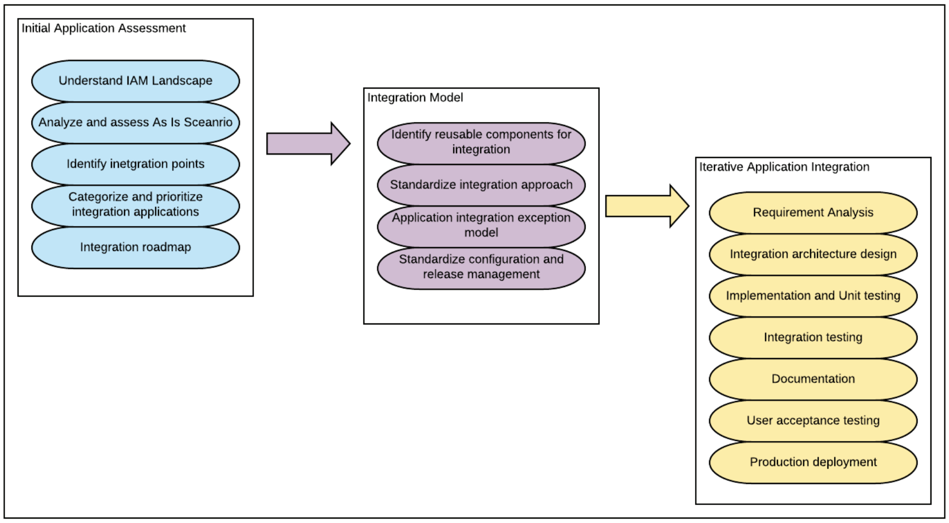
Application on-boarding on IAM platform is the stage in which the application is integrated with Oracle IAM for user provisioning and/or for authentication & authorization. Integration with following applications is included in current scope:

- Oracle EBusiness Suite
- Cook County Time (CCT)
- Integrated Property Tax System (Tyler Technologies Enterprise Assessment & Tax)
- Cherwell
- Agency(s) AD Forest (up to-5)
- Office 365
- Cisco VOIP
- CICO ISE
- Facility Access System
- Other Applications as identified (up to 5- 1 complex, 2 medium and 3 easy)[1]

Kapstone will leverage the “factory model” for on-boarding new applications on the IAM platform. The factory model constitutes automation of manual processes whenever possible and uses ready

[1] Complex – integration effort > 200 hours, Medium 100-200 hours, Easy < 100 hours

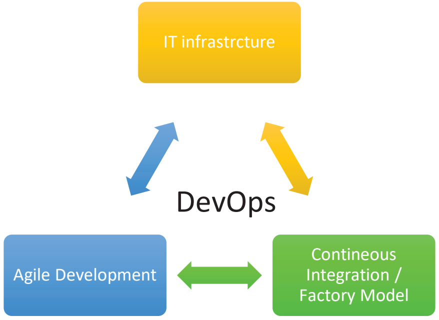
on-boarding templates with reusable code snippets, SDKs, extendible framework to integrate agency specific processes on the application side as demonstrated and further detailed in the illustration below.


Initial Application Assessment
Understand IAM Landscape
Analyze and assess As Is Sceanrio
Identify inetgration points
Categorize and prioritize integration applications
Integration roadmap
Integration Model
Identify reusable components for integration
Standardize integration approach
Application integration exception model
Standardize configuration and release management
Iterative Application Integration
Requirement Analysis
Integration architecture design
Implementation and Unit testing
Integration testing
Documentation
User acceptance testing
Production deployment

Each iteration of the factory model involves key activities like Design, Integration, Test, and Rollout and will follow the standard System Development Life Cycle (SDLC) phases.

Factory / Framework / Integration pattern

Kapstone's will adopt an agile methodology focused on time to value from strategy to implementation to operations. It leverages DevOps to enable predictable outcomes throughout.

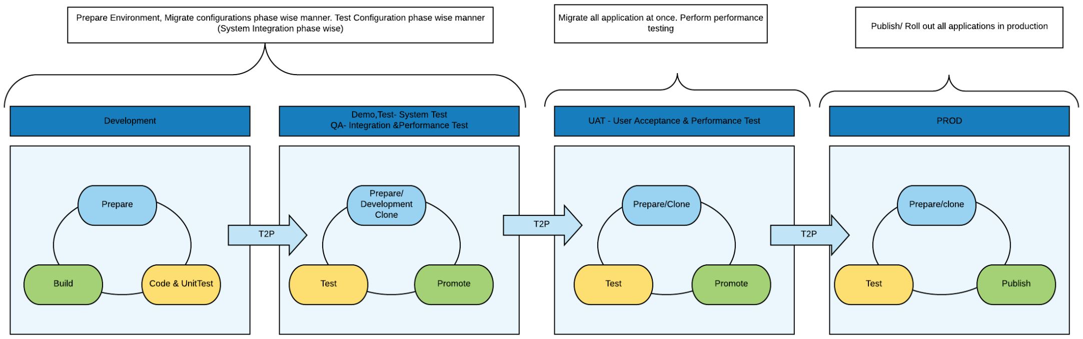


To ensure installation consistency and quality, the implementation procedures will be automated as much as possible. Silent installation and deploying pre-packaged applications will be used whenever appropriate.

The following diagram explains the required number of environment(s) and Kapstone's roll out plan across environments.

- Development – Environment will follow strategy to Build, code and perform unit testing for migrated code/application. Application will be on-boarded phase wise in development environment.

- Test, QA – Application on-board remains same as development environment (Phase wise manner) with additional testing like system integration testing, user acceptance testing and performance testing.
- UAT –This will act as pre-production environment. Once QA environment confirms code sanity, configuration will be finalized and simply on-board all application at once in this environment. Quick round of performance testing will be performed and integration testing to test sanity of environment.
- Production and DR – Actual roll out for application and switch over to new 12cPS4 system.


Prepare Environment, Migrate configurations phase wise manner. Test Configuration phase wise manner (System Integration phase wise)
Migrate all application at once. Perform performance testing
Publish/ Roll out all applications in production
Development
Demo,Test- System Test
QA- Integration &Performance Test
UAT - User Acceptance & Performance Test
PROD
Prepare
Build
Code & UnitTest
T2P
Prepare/ Development Clone
Test
Promote
T2P
Prepare/Clone
Test
Promote
T2P
Prepare/clone
Test
Publish

The central framework with the master user store will be expanded to include application-specific attributes in addition to the base profile. The user schema will be configured to identify the scope of the attributes. Application-specific attributes will be stored either in an external store or on the IAM user store. An attribute query service will be developed to return the application-specific attributes.

A sample schema for a multi-valued extension attribute design will be reviewed with county's stakeholders and will be configured. The extension attribute will be used to store application-specific attributes. Data can be stored in JSON or XML format. Access control will be implemented to return attributes that are in scope for an app.

```
{
            "id": "0001",
            "type": <saml / OIDC / Header>,
            "name": "Finance",
            "owner": “John Doe”,
            "attributes":
                        [{
                        "App1Attribute":
                                    [
                                    { "Name": "1001", "scope": <Regular/shared/global>,
                                    “Shared Apps” : [{ "id": "1002"},{"id": "1002"}]
                                    ]
                        }],
```

2.2.3. Topology and Architecture

Kapstone will install and configure OIAM as per Oracle's reference Deployment of Oracle Identity and Access Management with Microservices (in a Kubernetes Cluster) document, as referred in Appendix – B (reference architecture). Starting with Development environment till production, OIG implementation will follow clustered deployment as below:

- Database will be installed as RAC configuration on separate server.
- Node-1 OIAM: Admin server + OIM_Managed_Server1 + SOA_ Managed_Server1 + OAM_Managed_Server1.
- Node-2 to N: OIM_Managed_ServerN + SOA_ Managed_ServerN + OAM_Managed_ServerN.
- OIM N- Node: It Will be maintained in one OIM cluster.
- SOA N- Node: It will be maintained in one SOA cluster.
- OAM N- Node: It will be maintained in one OAM cluster.
- BI Servers will be installed separately and will support multiple OIM, OAM environments.
- Oracle HTTP servers in-front of OIM, OAM, SOA and BI clusters.
- Load balancer in-front of OIM cluster, SOA cluster, OAM cluster
- OIAM Version Assumptions.
- Supported OIAM versions: target: 12cPS4
- Supported Oracle Database "Enterprise Edition" versions.
- 12.1.0.2.0 onwards
    - CDB
    - Non-CDB
- All OIM, OAM schemas reside in same PDB within a CDB.
- Kapstone will deploy Oracle Identity and Access Management solutions on the. The containerized infrastructure will provide the failover capabilities to the OIAM environment and will be deployed in the County's secondary datacenter after the initial testing is complete.
- Oracle Linux will be used as the Operating System.
- These OIAM servers will leverage County's existing load balancer, DNS, Certificates, back-up and archival processes.
- Kapstone will build five environments: Development, Test/QA, Stage/UAT/Training, Production and Disaster Recovery (DR) Environment. The test/qa environment shall be created as baseline and then cloned for the Stage and Production Environment.
- Policy Management and Policy Studio: Oracle identity solution or PAM or other IAM solutions in don't follow any standard policy framework and each component keeps its policies in their respective stores. Oracle Identity governance related policies such as delegated administration, Approval workflows, provisioning workflows, Role based access, password policies, audit policies, user LCM policies are stored in database and can be reviewed using web interface. Similarly, Oracle Access management related policies like authentication,

authorization, audit policies are stored in databases and can be reviewed using web interface or using REST APIs.

2.2.4. Data Migration Approach

Kapstone will create a design document, that covers migration approach to perform upgrade from existing IAM solutions to OIAM 12cPS4 while minimizing downtime required for performing upgrade. This document will be shared with CCG. Kapstone will perform the upgrade by the Clean Slate approach.

During this stage, Kapstone will build new OIAM 12cPS4 and migrate IAM artefacts from existing Oracle IAM solution to new OIAM 12cPS4 using deployment manager, REST API policy migrations and Database operations. Customizations like authentication plug-ins, schedulers, event handlers, adaptor' metadata and jars will be migrated manually. All required adaptor configuration will need to be moved to new OIAM environment one by one application/connector wise. Migrate data using bulk load or recon process or using REST APIs.

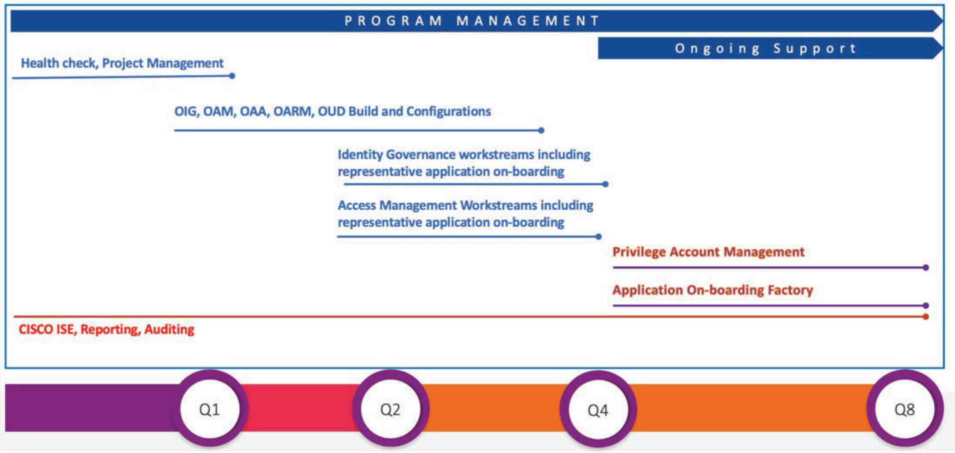
2.3. IAM Implementation Services

This section provides the IAM implementation services details.

2.3.1. Enterprise Identity & Access Management Implementation approach

Kapstone will execute IAM solution in multiple delivery streams. We will divide key areas into definable delivery work streams to better manage the project as a whole. The main benefit of this approach is the ability to understand dependencies, risks, and issues as they relate to the individual work streams as well as the broader project. Kapstone will undertake the work effort detailed in this proposal in discovery, health check and build phase workstream spanning over the period of 12 months. Year two will be focused on application on-boarding and refining IAM processes. Year three-five will be focused on optimizing run & operate processes.

The following figures depicts the project schedule with timing and sequencing of the overall engagement followed by breakdown of each phase:

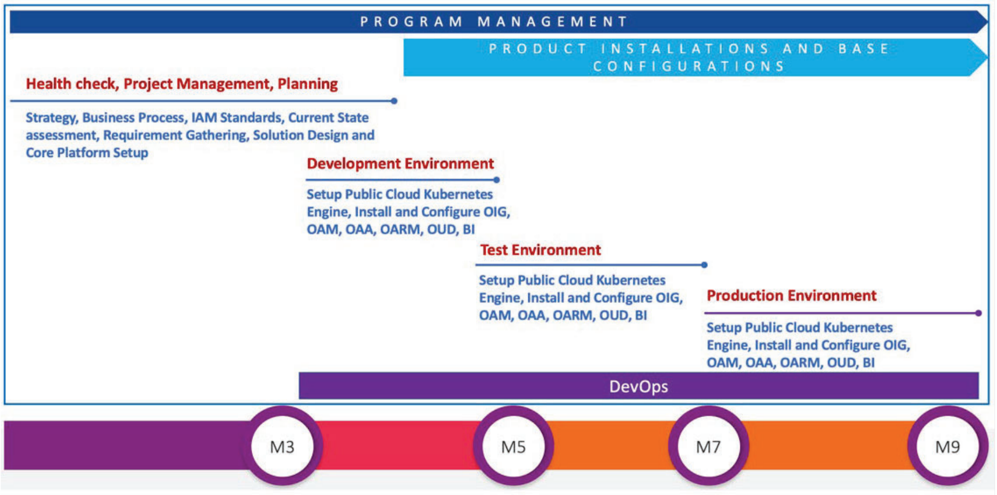

PROGRAM MANAGEMENT
Ongoing Support
Health check, Project Management
OIG, OAM, OAA, OARM, OUD Build and Configurations
Identity Governance workstreams including representative application on-boarding
Access Management Workstreams including representative application on-boarding
Privilege Account Management
Application On-boarding Factory
CISCO ISE, Reporting, Auditing
Q1
Q2
Q4
Q8

2.3.1.1. Phase 1 – Discovery, Design and Core Platform Set-up

- **Phase 1a: Discovery, Design**
- **Phase 1b: Core Platform Setup**

Kapstone will perform assessment for business processes to identify integration, authentication, authorization, provisioning, reconciliation, application on-boarding process, existing metadata maintenance process, approval workflows, access certifications, reports, auditing, data retention policies, business continuity plans, custom code for any business use case etc. relevant to implementation of EIAM in CCG's infrastructure. Kapstone will work CCG to review platform preference inclusive of cloud native technologies, DevOps, CICD, web server instances, managed servers, resources allotted to machines, databases, network configurations, hardware, and any tools used by CCG for building/installation of software as well as day to day maintenance of IAM solution. Based on information gathered during this process, Kapstone will develop an execution plan for future state of OIAM 12c and PAM for this project. Once the plan has been finalized, Kapstone will develop a roadmap to achieve future state and move to phase 2 of the projects.

The following figures depict the project schedule with timing and sequencing of phase 1 (Health check and build phase) of the engagement.


PROGRAM MANAGEMENT
PRODUCT INSTALLATIONS AND BASE CONFIGURATIONS
Health check, Project Management, Planning
Strategy, Business Process, IAM Standards, Current State assessment, Requirement Gathering, Solution Design and Core Platform Setup
Development Environment
Setup Public Cloud Kubernetes Engine, Install and Configure OIG, OAM, OAA, OARM, OUD, BI
Test Environment
Setup Public Cloud Kubernetes Engine, Install and Configure OIG, OAM, OAA, OARM, OUD, BI
Production Environment
Setup Public Cloud Kubernetes Engine, Install and Configure OIG, OAM, OAA, OARM, OUD, BI
DevOps
M3
M5
M7
M9

*M represents the month i.e., M3 – At the end of 3rd month of the engagement.

The focus of the Kapstone team will be to setup IAM framework, define & optimize security policies, setup standard application integration pattern to onboard applications onto the IAM platform as efficiently and effectively as possible. In order to do so, we will perform an upfront assessment to distribute the applications in scope based on level of effort, readiness, integration patterns, and dependencies.

Kapstone will establish a DevOps based deployment framework for achieving governance of Oracle IAM (OIG, OAM, OAA, OARM, OUD) deployments. DevOps process enables the organization to rapidly setup OIAM, because it can leverage reusable components developed between projects and develop automation templates for installation and initial build of base OIAM12c environment for different environments such as Test, UAT and Production in a consistent and repeatable process.

Using a framework increases productivity, improves quality and predictability; at same time achieves consistency in output.

2.3.1.2. Phase 2: Implementation (Build and Configure IAM Platform in DEV Environment)

Most enterprises have many applications that are integrated with an existing single sign on or authentication providers. Once of the key goal of deploying a new identity management system is to support a smooth transition business uses cases as they migrate onto the new system to consume new product features. The following goals will be met during the transition period:

- No negative impact to the business during transition
- Optimization of the identity management architecture in the new environment

Kapstone will build new OIAM 12cPS4 environment cleanly which will involve patching the environment to the latest bundle patch. The next step will be to setup OIG, OAM, OUD, OAA and OARM artifacts using Kapstone accelerators toolkit based on the final solution design. Once, the base infrastructure is available, user related data will be migrated using bulk load or recon process. OUD will be populated using OIG connector or using bulk import process.

Build and Configure IAM Platform in Development Environment

- Provision cloud services required for Development environment set-up as needed
- Set up base services controls, access, and connectivity.
- Build 12c OIM, OUD, OAM, OAA, OARM (OIAM) infrastructure with high availability following Oracle's best practices and documentation.
- Setup OIAM on containers using Containerization platform like Tanzu, OpenShift, OKE, EKS
- Enable TLS1.2+ protocol for secure communication.
- Create customizations as per the business functionality.
- Create a centralized policy management tool/framework, where possible, from design time to runtime for Identity Governance policies, request approval policies, access control policies, Identity Administrations policies, Authentication and Authorization policies.
- Setup integrations with IDPs - Azure AD and ADFS.
- Setup core common IAM services for authentication, authorization, application on-boarding, workflows, access controls, governance, compliance, and audit reporting.
- Integrate with HR authoritative source.
- Set up multi-factor authentication framework. Setup authentication orchestrations plug-ins that can be extendible to handle IP based restrictions, bring your own authentication, bring your own MFA, intranet access, VPN access and external facing application access.
- Setup Citizen / external user on-boarding interfaces (API framework, approval workflows, on-boarding processes, strong authentication enrollment, account verification / validation / proofing)
- Setup federation services, OAUTH, OIDC, SAML 2.0, Windows native authentications integration services on OIAM platform.
- Migrate identity data from the legacy platform inclusive of application domains, authentication and authorization modules, user, entitlement, roles, application instances, custom code, auditing data, certification data and additional workflow configurations.

- Migrate configurations and workflows from legacy platform.
- Implement archival and purging rules according to CCG's policies for data growth utilizing OOTB utilities provided by Oracle for archival, purging and compression of data.
- Integrate the new platform to send over the logs to log management tool that CCG uses.
- Create required reports.

Development and integration

Kapstone will categorize applications based on the inventory of web application and will also consider future applications. Kapstone will define applications on-boarding template for each integration category (Header variable based, cloud applications, SAML or OIDC based and others). Kapstone will provide its application owner self-service to define authorization group requirements, maintain service account credentials, provide / update SAML signing keys.

Kapstone will identify integration with target systems for provisioning and reconciliation as well as configure the Trusted source for OIG 12c. As part of deployment process the connector JARs and any relevant dependencies will be deployed on server. This will help prepare the server for configuration and migration of artifacts and user data.

User Data Management

User data will be migrated using bulk load tool available with OIAM 12c. This process will bring all user profile data, user account data, and any type of user child data to the new environment. Additionally, during this process role dependencies will be migrated. In addition, Kapstone will setup process to merge / consolidate user account data, map to centralized identity data, linked with social identities. Kapstone will also set up database and LDAP adapters on OUD to delegate password validation process.

Application Onboarding

Onboarding of applications is a process which enables IT and business owners to integrate applications with the OIAM solution to integrate them with the defined business processes and functions. Application owners work closely with the OIAM Application onboarding team to determine the appropriate integration pattern that will be applied for each individual application.

The onboarding processes will provide a simplified and consistent integration process for application teams using tools available OOTB with OIAM 12c and using Kapstone's application on-boarding toolkit and REST APIs.

Kapstone will establish an IAM on-boarding Factory to simplify and streamline the ongoing application integrations into the IAM solution.

IAM Migration Factory

Establishing an IAM Migration Factory, a dedicated team of skilled IAM resources who could rapidly deploy application integrations with IAM, in parallel also aligns well with the business requirements:

- Build and standardize application integration patterns that will rapidly scale to include new applications and provide documentation of the process to continue application onboarding after the engagement ends.
- Build and standardize the application onboarding process that can rapidly scale to include many applications in parallel and provide documentation on how to run the process after the engagement ends.

Deployment in Environments

- **Development –** Building a development environment will follow strategy to Build, code and perform unit testing for migrated code/application. Application will be on-boarded phases in development environment based on the strategy defined in the discovery process. Additionally, all previously mentioned steps will be performed to bring the environment to meet required business needs on user life cycle management and compliance.
- **Test–** The strategy for building development environment will be applicable for Test/QA environment too. All the steps will be executed, and in-addition system integration testing, and performance testing will be performed. Once the development environment confirms code sanity, configuration will be finalized and simply on-board all application at once in this environment. Performance testing will be performed and integration testing to test sanity of environment.
- **UAT –** The strategy for building development environment will be applicable for UAT environment too. All the steps will be executed, and in-addition user acceptance testing, and performance testing will be performed. This will act as pre-production environment. Once QA environment confirms code sanity, configuration will be finalized and simply on-board all application at once in this environment. Performance testing will be performed and integration testing to test sanity of environment.
- **Production and DR –** Actual rollout for application and based on cut-over strategy switch over to new 12cPS4 system. There will be a process defined for go-live as well as no-go strategy. Any of the go-live related processes that CCG expects Kapstone to follow will be identified as part of discovery and will be included in the strategy for go-live.
- **Deployment** - Kapstone will prepare and execute the deployment of the IAM platform in accordance with CCG's Change Management process, including:
    - Prepare Build and Deployment Guide.
    - Provide a Deployment Plan that outlines the activities that will occur prior to and immediately after Go Live, including Go/No-Go criteria.
    - Provide a Knowledge Transfer Plan for the transfer of knowledge necessary for CCG to properly operate and maintain the IAM Platform.
    - Execute Go Live, including documentation of a successful deployment and documentation of final acceptance of the solution by CCG.
    - Develop a Production Support Plan that addresses the post Go-Live support that will occur after Go Live.
    - Conduct project closeout & transition, which includes detailing the proposed schedule and activities associated with all transition tasks and turning over all relevant materials to CCG.

Identity Governance Implementation plan

Our recommended approach is to deliver the Identity Governance scope into three-waves.

IGA – Wave #1	IGA – Wave #2	IGA – Wave #3
• Building Identity Warehouse • RBAC / Birthright Access • Approval Workflows (Core Workflow and extendible framework to implement agency specific processes) • OIM Integration Interfaces	• User lifecycle management for the employees and contractors • User Access Certifications • Self-Service capabilities • Password Management • Delegated administration • Request based access provisioning, Custom (Agency Specific) Approvals, Escalations	• Ticketing System Integration • Role lifecycle management • Segregation of Duties

IGA - (User Life Cycle Management, Self-Service, Password Management, Delegated Administration, RBAC)
• Plan, design and implement employee on-boarding and off-boarding integration with HR and other authoritative sources and OIG.
• Plan, design and integrate AD, Azure AD, OUD, Agency applications with OIG.
• Configure and implement OIG as the user management interface with delegated administration and password management features.
• Configure OIM self-service password reset feature and leverage OIG as a framework to support custom password reset functionality.
• Plan, design and implement automated user access policies.
• Plan, design and implement self-service user access and resource request using OIG's OOTB shopping cart functionality.
• Plan, Design and Implement delegated administrations, multi-level approval workflows, multi-level provisioning workflows.
• Plan, Design and Implement access reviews and segregation of duties.
• Plan, Design and Implement Orphan / Rogue account management process.
• Plan, Design and Implement Service / System account management process.
• Enable OIG to generate ticket for hard resource requests (i.e., desktop phones, computers, etc.)
• Enable OIM's OOTB BI reports.

Access Management Implementation Plan

Most enterprises have many applications that are integrated with an existing access management system and/or homegrown access management components. A key goal of deploying a new access management system is to support a smooth transition for the legacy applications as they migrate onto the new system. The following goals will be met during the transition period:

- No negative impact to the business during transition
- Support for coexistence between the new and old environments
- Optimization of the access management architecture in the new environment

Access Management / Single Sign-On
• Plan, Analyze and design Access Management Platform to support on-premises and Cloud based web application.
• Integrate OAM with representative application of each category.
• Configure Multi-Factor Authentication using Oracle Mobile Authenticator, One time password token, Security challenge Question and Answers. Additionally, configure risk-based Authentication.
• Configure resilient pair of reverse proxy servers and setup web gates.
• Configure Authentication and Authorization policies, enable auditing and define.
• Plan, design and implement password polices and self-service for password management.
• Configure OUD and Setup multi-master replication to support HA. Integrate OUD with Database and AD/LDAP using adapters (Virtualizations).
• Enable OAM's OOTB BI reports.

2.3.1.3. Phase 3: Continuous Integrations and Application on-boarding / Migration

2.4.

Application Onboarding

Integrate with and up to eight other agency applications (to be identified during discovery phase). There are several ways to determine how applications will be prioritized for migration. Grouping typically will be done by integration pattern, criticality, and application readiness.

- Migrate existing application to target architecture integration patterns:
  - Header injection, J2EE Container security, Federation, OAuth, etc.
  - Applications often will change their integration pattern during migration.

Note - refer section 2.2 for the application on-boarding approach.

Privileged Access Management

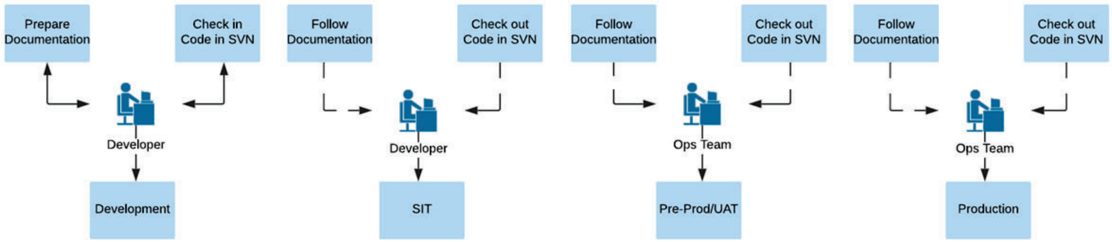
- Build and Configure Privileged Access Management Solution in up to 3 environments
- Integrate PAM with OIM and OAM
- Integrate OAM with up to 5 applications for password management.

Operational Support

Create and configure reports and analytics to assist in operations support and

- Perform proactive/preventive monitoring and to determine the solution critical path components of such activities as listed below:
  - Perform Root Cause Analysis, Developing custom tools/scripts where applicable.
  - Resolve Tickets
  - Monitor Systems availability
  - Set up notifications for system access breach
  - Conduct DR cycles
- Set up Alerts for
  - User activity, where user performs activities occasionally or ad hoc basis
  - For large query executions; Large import or export of files, data etc.
  - For high volume (by transaction count or transaction volume) activity by single user or single device or single location

Segregation of Duties during the Build Process



Kapstone understands that UAT and Production are controlled environments, and the deployment process requires segregation of duties. As a result, the build, Demo, Development, Test and QA environment will be built by Kapstone and the UAT and Prod or DR will be built by Kapstone jointly with CCG's Ops team. During the building of Development environment, Kapstone will prepare documentation and validate document by building Test and QA environment. Post QA build finalized document and code will be shared by Kapstone, with CCG's Ops team, for UAT, Prod and DR implementation.

Coexistence with current environment (ADFS or native authentication)

Coexistence enables Single Sign-On between the new Oracle access management environment and the current SSO product (ADFS, Azure AD). This is a common requirement during the migration phase to the new Oracle access management environment. There are several options to achieve coexistence including the following:

- Federation is an option for products that supports SAML or OIDC integration.
- Custom solutions shall be implemented if specific requirements need to be met.
- Need to determine which environment will handle password validation.
- Define how the environments will trust each other, i.e., 1-way or mutual trust.

NOTE: Clean-up and sun-setting old IAM environment post migration to new environment.

Load Balancer and Proxy Farm Approach, Azure Application Proxy, AWS ALB integration approach:

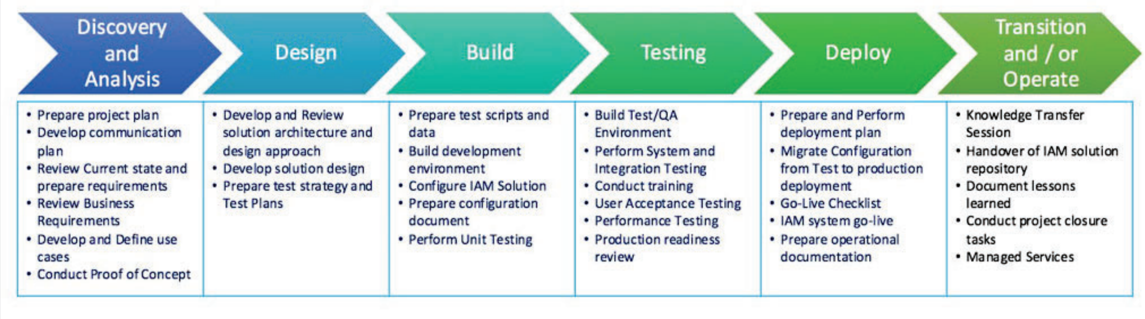
- Use of a proxy farm as a proxy solution.
- Use of Oracle HTTP Server (OHS) to front end the applications.
- 3-5 OHS servers can front-end several applications which previously will have had unique web gates

Policy Management

Oracle Access Manager admin interface or REST API can be used to setup and optimize authentication, Authorization, Multi-Factor authentication, Adapter access management / Zero-trust policies.

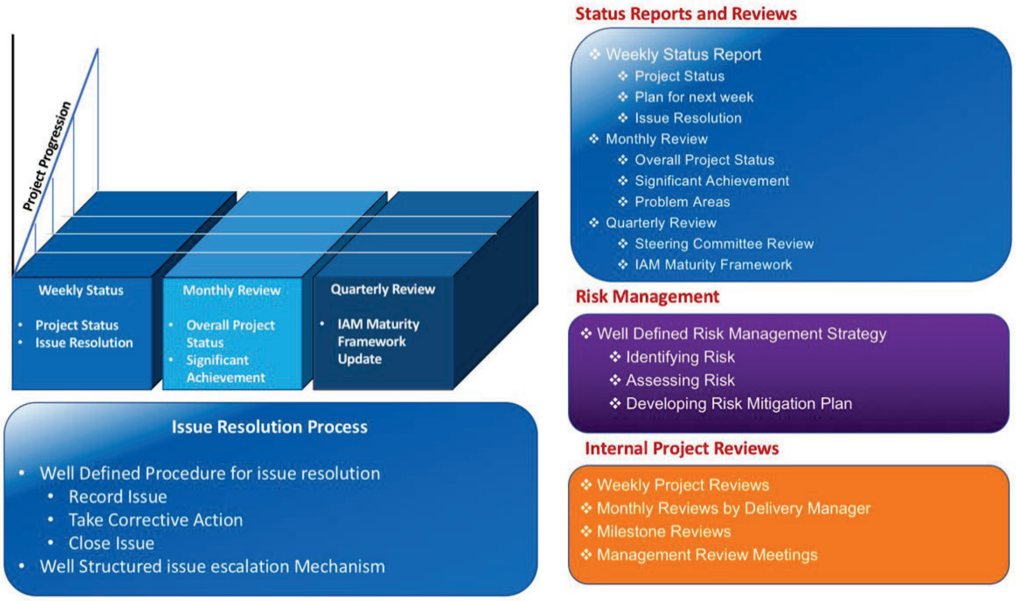
3. Project Implementation Methodology

Kapstone will deliver IAM project using the standard PMI Methodology, which defines a repeatable set of steps for solution delivery as below:



Discovery and Analysis	Design	Build	Testing	Deploy	Transition and / or Operate
• Prepare project plan • Develop communication plan • Review Current state and prepare requirements • Review Business Requirements • Develop and Define use cases • Conduct Proof of Concept	• Develop and Review solution architecture and design approach • Develop solution design • Prepare test strategy and Test Plans	• Prepare test scripts and data • Build development environment • Configure IAM Solution • Prepare configuration document • Perform Unit Testing	• Build Test/QA Environment • Perform System and Integration Testing • Conduct training • User Acceptance Testing • Performance Testing • Production readiness review	• Prepare and Perform deployment plan • Migrate Configuration from Test to production deployment • Go-Live Checklist • IAM system go-live • Prepare operational documentation	• Knowledge Transfer Session • Handover of IAM solution repository • Document lessons learned • Conduct project closure tasks • Managed Services

Kapstone's Project Management methodology will involve the following governance model for the project:



Weekly Status
- Project Status
- Issue Resolution

Monthly Review
- Overall Project Status
- Significant Achievement

Quarterly Review
- IAM Maturity Framework Update

Issue Resolution Process
- Well Defined Procedure for issue resolution
  - Record Issue
  - Take Corrective Action
  - Close Issue
- Well Structured issue escalation Mechanism

Status Reports and Reviews
- Weekly Status Report
  - Project Status
  - Plan for next week
  - Issue Resolution
- Monthly Review
  - Overall Project Status
  - Significant Achievement
  - Problem Areas
- Quarterly Review
  - Steering Committee Review
  - IAM Maturity Framework

Risk Management
- Well Defined Risk Management Strategy
  - Identifying Risk
  - Assessing Risk
  - Developing Risk Mitigation Plan

Internal Project Reviews
- Weekly Project Reviews
- Monthly Reviews by Delivery Manager
- Milestone Reviews
- Management Review Meetings

3.1. Project Management, Health check and scope management

Project And Scope Management
Kick off the project by understanding the existing business processes for Access Management, Identity Governance, and Identity Lifecycle management. Request and review key documents (Vision Statement, Project Charter, Scope).
Document CCG To-Be Architecture in collaboration with CCG which includes infrastructure requirements needed to support the current and future EIAM high availability and sizing requirements
Document the implementation roadmap in collaboration with CCG to enable EIAM services for adoption based on CCG priorities

Document Project Management Plan document which describes Kapstone's approach to managing the project along with a detailed project plan
Document the Requirements Management Plan which includes how we manage the requirements across all the workstreams by stating scope of key activities like Fit Gap Analysis to adjust and finalize the requirements as relevant at the beginning of each work stream, Test Management Plan
Document Test Plan to describe our test management approach which includes: • Requirements and disposition • All testing types such as installation verification (smoke test), functionality, performance/load testing, vulnerability testing, penetration testing and code tests • Vulnerability testing, penetration testing and code tests • Address test data requirements including test data generation • Test Scripts mapped to requirements • Defect Management • Release Management • Reporting

3.2. Product Build and Configuration

Product Build and Configuration
Finalize the public cloud platform and cloud native technologies. Validate the infrastructure and request necessary access to initiate the Product installation
Validate access and configure the DevOps scripts necessary to install the selected products
Download the necessary installable and initiate the installation (DevOps or Manual) in Development environment
Validate the installation for each product and document the build instructions
Document As Built document (server hostnames, ports, URLs, etc.)
Set up basic configuration to validate the integrations (optional)
Get environment signoff from CCG
Install and configure the finalized list of Authentication protocols, Authentication & Authorization modules, OIG connectors, Email Drivers, MFA Factors (SMS Provider)
Repeat above steps in QA, Prod and Prod HA in a clustered mode for applicable products

3.3. Project Testing Strategy

Kapstone shall create a testing strategy and plan for IAM platform. All components shall be unit tested prior to system integration testing. Kapstone shall perform the System Integration testing and assist the CCG in conducting the User Acceptance Testing. The IAM project shall conduct multiple rounds of testing as described in the table below:

Unit Testing	Any custom program (environment, interfaces, UIs, reports, extensions, data conversions, and other customizations) will be unit tested by the Kapstone team.
System Integration Testing	System integration testing is one of the most critical parts of an implementation project. Integration testing will test the complete set of the County's processes. Kapstone shall conduct the integration testing project's combined Kapstone-CCG technical team. Actual results shall be

	documented by Kapstone and compared to the expected results to ensure the business processes are working according to the design.
User Acceptance Testing	The end result of the process will be a preliminary acceptance of the systems, that will be done as User Acceptance Testing by the CCG team. All issues will be documented and will be reviewed with the County Team. When the testing has been completed, a meeting with all the appropriate individuals is conducted to make the final 'Go/No Go' decision for the implementation project
Stress Testing	Kapstone team shall conduct a non-automated testing on the system to measure and predict system performance against normal, anticipated loads, and further test the system's ability to sustain a high level of activity.
Security Audit	The CCG, at its sole discretion, may conduct an audit to verify that the system incorporates security and privacy standards as set forth in this agreement. If the County elects to conduct an audit, the Bureau of Technology and Information Security Office will deliver their joint findings to the project team. The project team will cooperate with the Bureau of Technology and Information Security Office to incorporate any change within scope recommended as a result of the County audit.

3.4. Issue Management

The project management team shall continually review all open issues and shall maintain an active log of issues including people issues, process issues, system issues, information security issues, infrastructure issues, patches and patch-sets with product vendors. Issues will be defined and logged by the project team and classified as system, business flow, infrastructure or others in order to streamline the resolution process. As part of the issue resolution process, each issue shall be categorized by severity and type, and assigned an owner.

3.5. Risk Management

Kapstone shall manage project risks in working with CCG and shall look for the opportunities to prevent and mitigate risks, a risk log shall be maintained for the project by the Project Manager. The Project Steering Committee shall serve as the primary risk management and review board. On an on-going basis, Project Governance Team (Kapstone and CCG) shall review all open issues and identify those that will impact the overall project.

Kapstone implementing an iterative, broadly applicable method mitigates requirements mismatch to reduce project risk. A key focus of each iteration in Kapstone project methodology is to identify and reduce the most significant project risks. This allows for the most critical risks to be addressed as early as possible in the project lifecycle, which results in a measurable reduction of schedule and budget risks.

Risk	Impact	Risk Mitigation
Non-availability / Schedule Constraint of Key Stakeholders from customer	Cause delay of deliverables	By listing all the dependencies, identifies stakeholders involved, and plan meetings in advance with required agenda Also having the customer Project Manager work with Kapstone team to assist in ensuring the required time can be made available from the intended stakeholder

Uncontrolled scope increase	Severely affects the project plan and objectives	Proposed changes to scope will go through scope control and needs approval of both implementer / vendor customer Project management team before inclusion. Introducing proper change management controls and procedure or toll gates will reduce the scope creep. Also, documenting the impact of changing requirements in terms of function points, time delays or cost implications help reduce the risk.
Non-availability of environments, support from Customer and required user access	Results in Schedule delays	In case of unavoidable delays in provisioning support, Kapstone worked on other independent components of the program Hardware and Software must be procured and made available to the implementation team well before the actual implementation starts, in-order to avoid any kind of delay in the delivery timeline.
Slippage in services / deliveries leading to increased cost	This will increase the cost of the project	Kapstone along with customer jointly assess the status of the project against the deliverables schedule on a weekly and monthly scale. Any deviations and inclusions outside the stated deliverables schedule will follow an escalation process
Insufficient/ Inappropriate documentation	Will hamper development and lead to errors	Do the minimum required documentation of the key processes within available time. Do application health check for documentation and fill shortage
Employee Turnover	Key personnel leave the project that might significantly delays or derails the project	By way of increased collaboration and information sharing within the team along with other best practices like common code ownership, regular review meetings (daily stand-ups, weekly or scheduled meetings) the risk due to employee turnover is small. Also working in an engaging, rewarding, empowered, collaborative environment people also helped us in mitigating this risk

3.6. Change Management

Kapstone shall develop a change management strategy to facilitate a smooth transition for IAM implementation. To support technology and business process change and their potential impacts, Kapstone's Project Manager will be responsible for assisting CCG in the following activities:

- Change impact analysis and document the findings.
- Identify organizations and work groups that will be most impacted by technology and business process changes.
- Determine the change impact to organization and groups.

- Assist with documenting and communication of changes.
- Create transition (support) plans to manage the impacts of the project.

3.7. Communication Strategy

Kapstone shall assist CCG in developing a communication strategy/plan. The CCG will utilize this strategy and effectively communicate with the stakeholders to ensure that they have a clear understanding of the functionality and the associated benefits being deployed, impact on the data collection/exchange and the timing of the implementation.

The communication plan can assist with ensuring that the stakeholders can:

- Understand the objectives of the project.
- Be aware of the likely impact of the project.
- Get periodic status updates.
- Know where and how to obtain information about the project.
- Provide feedback.

3.8. Training

Kapstone shall be responsible for creating a CCG-specific training plan and providing training using the Train-The-Trainer method. The training material can either be in a Microsoft Word/PowerPoint format which may be editable for CCG's future use. The CCG Manager, or their designate, will review and approve all training material prior to its delivery. Training will be performed as Virtual using the Microsoft Team.

Training Task	Responsibility		Comments
	CCG	Kapston e	
Plan Training		ü	
Create Training Material		ü	
QA Training Material		ü	
Review/Approve Training Material	ü		According to pre-defined criteria
Deliver Train-The-Trainer Training (Technical Training)		ü	Deliver Initial Training to County SME/Lead
Plan and Deliver End User Training	ü		Deliver End User Training
Schedule Training	ü		Students, Rooms, Sessions

Train-The-Trainer Training shall include the following Technical Training and the hours.

#	Course Name	Est. Training Hours
1	IAM Platform	8
2	IGA Implementation	8
3	Access Management Implementation	8

4	Others (Open Ended as needed)	8
Total Training Hours		**32**

5. Project Schedule.

The following is the preliminary project schedule. This will be revised in consultation with the CCG project manager at the start of the project. The project start date is contingent on approval of the County Board.

WBS	Task Name	Duration	Start	Finish
	Cook County - Enterprise Identity and Access Management (EIAM) Project	549d	3/5/2024	4/10/2026
1.1	Phase I (Installation, Configuration EIAM Platform and IGA trusted source and key target configurations & five SSO Application on-boarding as Pilot)	293d	3/5/2024	4/17/2025
1.1.1	Definition	34d	3/5/2024	4/19/2024
1.1.1.1	Project Initiation and Planning	24d	3/5/2024	4/5/2024
1.1.1.1.1	Define Project Governance Structure	5d	3/5/2024	3/11/2024
1.1.1.1.1.1	Status Reporting and Monitoring	5d	3/5/2024	3/11/2024
1.1.1.1.1.2	Issue Reporting and Escalation	5d	3/5/2024	3/11/2024
1.1.1.1.1.3	Risk Analysis and Management	5d	3/5/2024	3/11/2024
1.1.1.1.1.4	Communication Management	5d	3/5/2024	3/11/2024
1.1.1.1.1.5	Plan Project Kick-Off	5d	3/5/2024	3/11/2024
1.1.1.1.2	Review Project Scope and Deliverables	10d	3/18/2024	3/29/2024
1.1.1.1.2.1	Review Project Management Methodology	10d	3/18/2024	3/29/2024
1.1.1.1.2.2	Create High-Level Project Work Plan	10d	3/18/2024	3/29/2024
1.1.1.1.2.3	Review Deliverables and Timeline	10d	3/18/2024	3/29/2024
1.1.1.1.2.4	Identify Project Org Chart	10d	3/18/2024	3/29/2024
1.1.1.1.2.5	Review Roles and Responsibilities	10d	3/18/2024	3/29/2024
1.1.1.1.2.6	Identify Repository for Project Deliverables	10d	3/18/2024	3/29/2024
1.1.1.1.3	Change Management and Training Strategy	5d	3/18/2024	3/22/2024
1.1.1.1.3.1	Identify Change Management Strategy	5d	3/18/2024	3/22/2024
1.1.1.1.3.2	Confirm Training Strategy	5d	3/18/2024	3/22/2024
1.1.1.1.4	Create Project Charter	5d	4/1/2024	4/5/2024
1.1.1.1.4.1	Implementation Strategy	5d	4/1/2024	4/5/2024
1.1.1.1.4.2	Communication Strategy	5d	4/1/2024	4/5/2024
1.1.1.1.4.3	Change Management Strategy	5d	4/1/2024	4/5/2024
1.1.1.1.4.4	Risk Mitigation Strategy	5d	4/1/2024	4/5/2024

1.1.1.2	Review and Approve Project Charter	2d	4/7/2024	4/8/2024
1.1.1.3	Review & Approve Plan	2d	4/7/2024	4/8/2024
1.1.1.4	Infrastructure	10d	4/8/2024	4/19/2024
1.1.2	M: Project Charter Approved	0	4/8/2024	4/8/2024
1.1.3	M: Project Plan Approved	0	4/8/2024	4/8/2024
1.1.4	Requirement Analysis	51d	4/22/2024	7/1/2024
1.1.4.1	Project Kick-Off	4d	4/22/2024	4/25/2024
1.1.4.1.1	Conduct Project team Orientation	1d	4/22/2024	4/22/2024
1.1.4.1.2	Conduct Project Kick-Off Meeting	2d	4/22/2024	4/23/2024
1.1.4.1.3	Conduct Organizational Kick Off	2d	4/24/2024	4/25/2024
1.1.4.2	Assessment - Pilot Application Integration for IGA and SSO	40d	5/7/2024	7/1/2024
1.1.4.2.1	Application Architecture Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.2	SSO, Directory services and MFA Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.3	SSO method Support Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.4	Identity LCM, Approval workflows and Governance Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.5	PAM and ISE Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.6	Citizen Identity and Self-Service Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.7	Security Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.8	Compliance Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.9	3rd Party Integrations Requirements	40d	5/7/2024	7/1/2024
1.1.4.2.10	Auditing and Reporting Requirements	40d	5/7/2024	7/1/2024
1.1.4.3	Infrastructure Requirements - EIAM Platform	15d	4/22/2024	5/10/2024
1.1.4.3.1	Hardware Requirements	15d	4/22/2024	5/10/2024
1.1.4.3.2	Physical Environment Requirements	15d	4/22/2024	5/10/2024
1.1.4.3.3	Network Requirements	15d	4/22/2024	5/10/2024
1.1.4.3.4	Business Continuity and Disaster Recovery	15d	4/22/2024	5/10/2024
1.1.4.3.4	Business Continuity and Disaster Recovery	15d	4/22/2024	5/10/2024
1.1.4.3.5	Hardware and Software Licensing / Warranties	15d	4/22/2024	5/10/2024
1.1.4.3.6	Auditing Requirements	15d	4/22/2024	5/10/2024
1.1.4.4	Operations & Support Requirements	15d	5/21/2024	6/10/2024
1.1.4.4.1	Product Support & Transition	15d	5/21/2024	6/10/2024
1.1.4.4.2	Defect Resolution & Solution Acceptance	15d	5/21/2024	6/10/2024

1.1.4.4.3	Solution Administration	15d	5/21/2024	6/10/2024
1.1.4.4.4	Solution Management	15d	5/21/2024	6/10/2024
1.1.4.5	Creation EIAM Implementation Roadmap	10d	6/10/2024	6/21/2024
1.1.4.6	Create EIAM Administration Best Practices	10d	6/10/2024	6/21/2024
1.1.5	M: Requirement Specification Document Created	0	6/10/2024	6/10/2024
1.1.6	M: EIAM Infrastructure Design Completed	0	7/2/2024	7/2/2024
1.1.7	M: EIAM Implementation Roadmap Created	0	6/23/2024	6/23/2024
1.1.8	M: Pilot application integration / on-boarding Implementations Requirement template Created	0	6/23/2024	6/23/2024
1.1.9	Solution Design	55d	6/17/2024	8/30/2024
1.1.9.1	Design Best Practice and Standards	15d	6/24/2024	7/12/2024
1.1.9.1.1	Architecture Goals	15d	6/24/2024	7/12/2024
1.1.9.1.2	Application Integration Standards	15d	6/24/2024	7/12/2024
1.1.9.1.3	Design Principles	15d	6/24/2024	7/12/2024
1.1.9.1.4	Design Patterns	15d	6/24/2024	7/12/2024
1.1.9.1.5	EIAM Platform Solution Design	15d	6/24/2024	7/12/2024
1.1.9.1.6	Pilot Application Integration Solution Design	15d	6/24/2024	7/12/2024
1.1.9.2	Technical Design - EIAM Platform	20d	8/5/2024	8/30/2024
1.1.9.2.1	Physical Architecture Design	20d	8/5/2024	8/30/2024
1.1.9.2.2	Access Management Design	20d	8/5/2024	8/30/2024
1.1.9.2.3	Database Design	20d	8/5/2024	8/30/2024
1.1.9.2.4	Storage Design	20d	8/5/2024	8/30/2024
1.1.9.2.5	Resources Design	20d	8/5/2024	8/30/2024
1.1.9.2.6	Integration Points Design	20d	8/5/2024	8/30/2024
1.1.9.2.7	Notifications Design	20d	8/5/2024	8/30/2024
1.1.9.2.8	Network Design	20d	8/5/2024	8/30/2024
1.1.9.2.9	Project Management	20d	8/5/2024	8/30/2024
1.1.9.2.10	Perform Quality Assurance	4d	8/5/2024	8/8/2024
1.1.9.3	Solution Design - Pilot Application Integration	40d	6/17/2024	8/9/2024
1.1.9.3.1	SSO App Integration Specifications, Trusted & Target application integration for IGA	35d	6/24/2024	8/9/2024
1.1.9.3.2	Application Attribute Mapping, OUD Schema Configurations, OIM UDF Configurations, OAM Policy Attribute mapping	35d	6/17/2024	8/2/2024
1.1.10	M: Technical Design Completed	0	8/30/2024	8/30/2024
1.1.11	M: Pilot Integration Pattern Design Completed	0	8/30/2024	8/30/2024

1.1.12	Build	80d	9/2/2024	12/20/2024
1.1.12.1	EIAM Platform Build	59d	9/2/2024	11/21/2024
1.1.12.1.1	Build Source Control and Continuous Integration Environments	5d	9/2/2024	9/6/2024
1.1.12.1.2	Platform Installation - DEV	35d	9/9/2024	10/25/2024
1.1.12.1.2.1	Hardware Installation	10d	9/9/2024	9/20/2024
1.1.12.1.2.2	Software Installation	10d	9/22/2024	10/3/2024
1.1.12.1.2.3	Configuration	10d	10/7/2024	10/18/2024
1.1.12.1.2.4	Testing	5d	10/21/2024	10/25/2024
1.1.12.1.3	Platform Installation - TEST / QA / STAGE	19d	10/28/2024	11/21/2024
1.1.12.1.3.1	Software Installation	5d	10/28/2024	11/1/2024
1.1.12.1.3.2	Configuration	10d	11/3/2024	11/14/2024
1.1.12.1.3.3	Testing	5d	11/17/2024	11/21/2024
1.1.12.2	Build - Application Integration Pattern	80d	9/2/2024	12/20/2024
1.1.12.2.1	Develop SSO and IGA On-boarding Integration patterns	80d	9/2/2024	12/20/2024
1.1.12.2.2	Develop Services	80d	9/2/2024	12/20/2024
1.1.12.2.3	Develop Business Process	80d	9/2/2024	12/20/2024
1.1.12.2.4	Apply Security	80d	9/2/2024	12/20/2024
1.1.12.2.5	Develop Policies, Workflows, Scheduled tasks, Event handlers, AuthN plug-ins, AuthZ plug-ins	80d	9/2/2024	12/20/2024
1.1.13	M: DEV Environment Created	0	10/25/2024	10/25/2024
1.1.14	M: TEST Environment Created	0	11/22/2024	11/22/2024
1.1.16	Testing	115d	9/2/2024	2/7/2025
1.1.16.1	Develop Testing Strategy and Plan	15d	9/2/2024	9/20/2024
1.1.16.2	Create System Test Cases	30d	9/22/2024	10/31/2024
1.1.16.3	Conduct System Integration Testing	40d	11/24/2024	1/16/2025
1.1.16.4	Conduct Load Test	5d	1/20/2025	1/24/2025
1.1.16.5	Conduct System Stress Testing	5d	1/20/2025	1/24/2025
1.1.16.6	Conduct User Acceptance Testing - UAT	15d	1/20/2025	2/7/2025
1.1.17	M: Test Strategy Created	0	9/20/2024	9/20/2024
1.1.18	M: Test Cases Developed	0	11/1/2024	11/1/2024
1.1.19	M: System Testing Completed	0	1/17/2025	1/17/2025
1.1.20	M: Load and Stress Testing Completed	0	1/24/2025	1/24/2025

1.1.21	M: UAT Completed	0	2/6/2025	2/6/2025
1.1.22	Training and Transition	46d	11/3/2024	1/3/2025
1.1.22.1	Prepare Training Environment	5d	11/3/2024	11/7/2024
1.1.22.2	Prepare Training Materials	20d	11/10/2024	12/5/2024
1.1.22.3	Review and Approve Training Materials	10d	12/9/2024	12/20/2024
1.1.22.4	Conduct End User Training	5d	12/23/2024	12/27/2024
1.1.22.5	Conduct Technical User Training	5d	12/30/2024	1/3/2025
1.1.23	M: Training Materials Prepared	0	12/6/2024	12/6/2024
1.1.24	M: Training Completed	0	1/3/2025	1/3/2025
1.1.25	Production Deployment	26d	3/13/2025	4/17/2025
1.1.25.1	Prepare for Production	5d	3/13/2025	3/19/2025
1.1.25.1.1	Assess Production Readiness	5d	3/13/2025	3/19/2025
1.1.25.1.2	Review Support Plan	5d	3/13/2025	3/19/2025
1.1.25.1.2.1	Review and Update Help Desk and Delegated Administration Strategies	5d	3/13/2025	3/19/2025
1.1.25.2	Production Implementation	18d	3/13/2025	4/7/2025
1.1.25.2.1	Platform Installation - DR	15d	3/13/2025	4/2/2025
1.1.25.2.2	Platform Installation – PROD	15d	3/13/2025	4/2/2025
1.1.25.2.3	Prod and DR Regression Testing	5d	4/1/2025	4/7/2025
1.1.25.3	GO-Live	5d	4/11/2025	4/17/2025
1.1.26	M: Production Implementation Plan Created	0	2/13/2025	2/13/2025
1.1.27	M: DR Environment Created	0	4/17/2025	4/17/2025
1.1.28	M: PROD Environment Created	0	4/17/2025	4/17/2025
1.1.29	M: Production Configuration (GO LIVE) Completed	0	4/17/2025	4/17/2025
1.2	Phase II (Application Integration Implementation)	257d	4/17/2025	4/10/2026
1.2.1	SSO and IGA Application Integration - Iteration #1	65d	4/17/2025	7/16/2025
1.2.2	SSO and IGA Application Integration - Iteration #2	65d	7/16/2025	10/14/2025
1.2.3	SSO and IGA Application Integration - Iteration #3	65d	10/14/2025	1/12/2026
1.2.4	SSO and IGA Application Integration - Iteration #4	65d	1/12/2026	4/10/2026
1.3	Post Go-Live Support		4/11/2025	

6. Project Deliverables.

The following table includes key project deliverables for the IAM implementation at CCG.

Table: List of Deliverables

#	Deliverable	Phase (1, 2 or 3/other)
6.001	Project Charter	1
6.002	Project Plan Approved	1
6.003	Requirement Specification Document Created	1
6.004	Infrastructure Design Completed	1
6.005	Technical Design Completed	1
6.006	Dev Env Created	2
6.007	QA Env Created	2
6.008	Test Strategy and Plan Created	2
6.009	Test Cases Developed	2
6.010	System Testing Completed	2
6.011	UAT Completed	2
6.012	PROD Environment Created	2
6.013	Production Go-Live	2
6.014	DR Environment Completed	2
	Iteration 1	
6.015	Dev Env Updated	3
6.016	Test Env Updated	3
6.017	SIT Completed	3
6.018	UAT Completed	3
6.019	Production Go-Live	3
	Iteration 2	
6.020	Dev Env Updated	3
6.021	Test Env Updated	3
6.022	SIT Completed	3
6.023	UAT Completed	3
6.024	Production Go-Live	3
	Iteration 3	
6.025	Dev Env Updated	3
6.026	Test Env Updated	3
6.027	SIT Completed	3
6.028	UAT Completed	3
6.029	Production Go-Live	3
	Iteration 4	
6.030	Dev Env Updated	3
6.031	Test Env Updated	3
6.032	SIT Completed	3
6.033	UAT Completed	3
6.034	Production Go-Live	3

6.035	Support Transition Completed	3

6.1. Deliverable Definition and Acceptance Criteria

The table that follows provides the expected content and completion criteria of the deliverables required for the CCG's Enterprise Identity & Access Management Implementation project. For all the deliverables outlined in the below table, the common acceptance criteria will be a sign off by CCG Project Manager or a representative from CCG designated by CCG project manager.

#	Category	Deliverable	Phase	Description	Format	Completion Criteria
6.001	Planning and Design	Project Charter	1	Conduct Project Kick-off meeting and provide an overview of • Project Scope • Project Schedule Provide guidelines on how the County and Kapstone will work together to achieve the common project objectives. Kapstone and County PM's will work together to develop project governance. The deliverable material includes: • Project Management Approach • Project Organization chart • Project Methodology • Issue Management Approach • Project Status Approach • Change Management Approach • Risk	Microsoft Word	County Provides the approval of the document

				Management Approach • RAID (risks, assumptions, issues and dependencies) logs		
6.002	Planning and Design	Project Plan Approved	1	Defines the efforts and resource planning for project	Microsoft Project / Excel or County Provided Project Management tool	County Provides the approval of the document
6.003	Planning and Design	Requirement Specification Document Created	1	Capture customer functional and non-functional requirements	Microsoft Word	County Provides the approval of the document
6.004	Planning and Design	Infrastructure Design Completed	1	This deliverable includes design of the integration of all the technology components that support EIAM platform	Microsoft Word	County Provides the approval of the document

6.005	Planning and Design	Technical Design Completed	1	This deliverable includes the data definition and data mapping for the functional design. The technical design is a refinement of the Integration Functional Design and specifies all the process, transformation, and architecture components in the integration solution to the lowest level of detail. This deliverables also include Integration Specification Document : Define strategy to define prioritization and logical clubbing of applications, which will be integrated with OIAM	Microsoft Word	County Provides the approval of the document

6.006	Build	Dev Env Created	2	The deliverable is complete when the instance is available for configuration and includes 1) Installation and configuration of the base Oracle IAM software in the Development environment 2) Updated Development Environment System Architecture 3) Summary of the configuration objects required to support the solution. Covers Product installation and configurations 4) Summary of configurations specific to application integration	Microsoft Word (Configuration Document including product installations and LDAP/user store integrations)	County Provides the approval of the document and confirm the completion of development environment
6.007	Build	QA Env Created	2	The deliverable is complete when the instance is available for configuration and includes 1) Installation and configuration of the base Oracle IAM software in the QA environment 2) Updated Development Environment	Microsoft Word (Configuration Document including product installations and LDAP/user store integrations)	County Provides the approval of the document and confirm the completion of Test / QA environment

				System Architecture 3) Summary of the configuration objects required to support the solution. Covers Product installation and configurations 4) Summary of configurations specific to application integration		
6.008	Planning and Design	Test Strategy and Plan Created	2	Defines the approach for testing the solution, creating test conditions, scripts, and expected results, and defines test cycles for the tests, pass/fail criteria, performance, etc. Defines the scenario for each test along with the expected result for each of the testing stages. A test script details the exact steps that a tester will follow to complete testing (i.e., to test all the conditions). The Test Plan content will include: o Testing Strategy Approach o Test Plan	Microsoft Word	County Provides the approval of the document

				o Test Data Setup Document o Testing Responsibilities o Testing Environments o Regression Test Plan		
6.009	Testing	Test Cases Developed	2	Test scripts authored and approved to ensure the full system is appropriately tested against Assist the County to create test scripts to support the testing. • Test cases; • Unit Test Cases;	Microsoft Word	County Provides the approval of the document
6.010`	Testing	System Testing Completed	2	Plan and execute System Integration Testing The deliverable includes: • Perform System Integration Testing according to Plan using Test scripts • Create Test Data Compare results against	Microsoft Word	County Provides the approval of the document

				expected results pass/fail and findings • Document Issues for retesting in the next round • Test Results		
6.011	Testing	UAT Completed (Also include UAT env created and, Training Materials, Train-The-Trainer Training Delivered)	2	Build UAT environment and Plan and execute User Acceptance Testing. The deliverable will include: • Perform User Acceptance Testing according to plan using test scripts • Compare results against expected results and document pass/fail and findings • Test Results The deliverable will also include: • Training materials • Conduct "Train-The-Trainer" training Classes for County Users • Conduct Training Classes for Technical Team - Administrator	Microsoft Word	County Provides the approval of the document

6.012	Build	PROD Environment Created and Production cutover plan	2	The deliverable is complete when the instance is available for configuration and includes 1) Installation and configuration of the base Oracle IAM software in the Production environment 2) Updated Development Environment System Architecture 3) Summary of the configuration objects required to support the solution. Covers Product installation and configurations 4) Summary of configurations specific to application integration The deliverable will include a production cutover plan and list the tasks, resource and timeline for production deployment - Covers data migration strategy • Go live Implementation Plan The Cutover Plan contains specific	Microsoft Word	County Provides the approval of the document

				deployment tasks, dates, assignments, and dependencies for each Release deployment detailing migration processes. Cutover Plan and checklist outline the activities planned for that are required for transition from application specific security mechanism to centralized, OIAM based authentication infrastructure and provide an ability to keep track of those activities. The Cutover Checklist contains specific work items and dependencies for each Release deployment to provide an ability to keep track of those items.		

6.013	Deploy	Production Go-Live	2	The deliverable will include: • Production Configuration Complete • Production Validation Complete • Production System made available to users • Updated System Maintenance and Support Document • Deployment Document; • Regression Testing Results	Microsoft Word	County Provides the approval of the document
6.014	Deploy	DR Environment Completed	2	The deliverable is complete when the instance is available for configuration and includes 1) Installation and configuration of the base Oracle IAM software in the DR environment 2) Updated Development Environment System Architecture 3) Summary of the configuration objects required to support the solution. Covers Product installation and configurations 4) Summary of	Microsoft Word	County Provides the approval of the document

				configurations specific to application integration		
		Iteration 1 (3 Months)				
6.015	Application On-boarding	Dev Env Updated	3	This deliverable includes on-boarding first batch of agency applications in development environment	Application on-boarded and update application on-boarding document, If needed	confirm the completion of the application on-boarding in scope
6.016		Test Env Updated	3	This deliverable includes on-boarding first batch of agency applications in TEST environment		
6.017		UAT Completed	3	This deliverable includes on-boarding first batch of agency applications in UAT environment		
6.018		Production Go-Live	3	This deliverable includes on-boarding first batch of agency applications in Production environment		

		Iteration 2 (3 Months)				
6.019		Dev Env Updated	3	This deliverable includes on-boarding second batch of agency applications in development environment		
6.020		Test Env Updated	3	This deliverable includes on-boarding second batch of agency applications in TEST environment		
6.021		UAT Completed	3	This deliverable includes on-boarding second batch of agency applications in UAT environment		
6.022		Production Go-Live	3	This deliverable includes on-boarding second batch of agency applications in Production environment		
		Iteration 3 (3 Months)				
6.023		Dev Env Updated	3	This deliverable includes on-boarding third batch of agency applications in development environment		
6.024		Test Env Updated	3	This deliverable includes on-boarding third batch of agency		

				applications in TEST environment		
6.025		UAT Completed	3	This deliverable includes on-boarding third batch of agency applications in UAT environment		
6.026		Production Go-Live	3	This deliverable includes on-boarding third batch of agency applications in Production environment		
		Iteration 4 (3 Months)				
6.027		Dev Env Updated	3	This deliverable includes on-boarding fourth batch of agency applications in development environment		
6.028		Test Env Updated	3	This deliverable includes on-boarding fourth batch of agency applications in TEST environment		
6.029		UAT Completed	3	This deliverable includes on-boarding fourth batch of agency applications in UAT environment		
6.030		Production Go-Live	3	This deliverable includes on-boarding fourth batch of agency applications in Production environment		

6.031		Support Transition Completed	3	The deliverable provides the operational procedures to run and maintain the access management system. This guide covers how to perform basic administrative tasks and system maintenance routines that need to be performed on an ongoing basis.	Microsoft Word	County Provides the approval of the document

6.2. Project Deliverables & Ownership

Listed below are the tasks involved during various phases of the project.

Project Phase	Primary Activities - Ownership	Deliverables - Ownership	Assumptions and High-Level CCG Resource requirements
Design	– Identify and list functional and non-functional requirements – Kapstone – Map functional requirement to technical requirement- Joint Ownership – Prepare the Project Architecture Roadmap - Kapstone – Prepare Design - Kapstone	– System Requirements Specification – Kapstone – Business Requirements Document– Joint Ownership – Detailed Project Plan - Kapstone – Detailed Design Document - Kapstone – Test strategy for the project – Joint ownership – Sign-off for Requirements Document and	– Kapstone team will CCG IAM team, Application Owners, Infrastructure Team, Security Team and other stake holders to review and validate business requirements. – Kapstone team will work with CCG infrastructure team to setup the demo environment, setup various credentials & network access and to setup ad-hoc and scheduled backup. – Kapstone will work with CCG Enterprise Architecture team and review solution architecture. Kapstone will work with CCG's Enterprise

		High-level Architecture documents – CCG	Architecture team to understand and map with current application environment and roadmap. – Kapstone team will work with CCG Business team to validate workshop environment.
Environment Setup	Setup OIG Repository, Application Servers– Kapstone Data clean-up – Joint Ownership	– OIG installed on 5 different environments starting with Development to Production environments – Kapstone	– CCG team will set up and provide the following as a pre-requisite for build: – Database – Hardware – Network Access – Load Balancer setting
Development / Configuration	Migrate OIG configuration like UDF, sandbox, lookups, custom schemas, custom codes, metadata, schedulers, event handlers, adapters - Kapstone Migrate Connectors based on priority and application grouping prepared during design session – Kapstone Reconcile data to OIM using Recon job – Kapstone Configure Audit and Reporting – Kapstone Perform Unit testing in Development Environment – Kapstone	– Development and configuration complete in Development environment – Kapstone – System Configuration/ Code Design Document – Kapstone	– Kapstone team will work with CCG stakeholders during integration
Testing	Perform System Integration testing on the code in the Development environment – Kapstone Perform User Acceptance testing on the QA environment – Joint (CCG, Kapstone) Perform performance testing – Joint (CCG, Kapstone)	– Test Plan – Kapstone – Integration Test Results – Kapstone – User Acceptance Test Results – Kapstone – User Acceptance Report - CCG	– Kapstone team will need active participation from the CCG stakeholders/ teams in this phase as well. – Integration testing will be performed phase wise. Application wise configurations will be migrated, and integration testing will be performed.

		– User Acceptance Test Sign-off – CCG	
UAT	Clone QA Environment using T2P – Kapstone Perform Performance tuning – Kapstone Perform performance testing - Joint (CCG, Kapstone)	– Test Plan – Kapstone – Integration Test Results – Kapstone – Performance Test Results – Kapstone – Performance Test Report - CCG – Performance Test Sign-off – CCG	– Kapstone team will need active participation from the application teams in this phase as well. – Performance testing will be performed with fully loaded OIM (all application migrated to OIM). It will identify if system can cater full load and if required any additional tuning for system, it can be performed.
Production Deployment	Work with CCG team to deploy the system in the Production Environment – Joint Ownership Assist CCG team in configuring and testing network firewall, proxy servers, Monitoring system - Joint Ownership Assist CCG team to prepare the go-live check lists – Joint Ownership Review the System Progress and perform initial validation -Joint Ownership Go-Live with all users and Perform final validation - Joint Ownership	– Migration/Systems validation results – Joint Ownership – Production Deployment document – Kapstone – Production Runbook – Kapstone – Final - User Acceptance report - CCG – GO-LIVE decision report - CCG – GO-LIVE results - CCG	– Kapstone will develop Environment LCM script and Kapstone consultant(s) will provide guidance to the CCG team for production deployment and support the effort which includes: – Code & Configuration Migration – Smoke Testing
Post-Production Support	Provide support for a period of 4 weeks for any potential issues arising from the OIG deployment - Kapstone Provide Administrator and End-User training to CCG regarding the maintenance of the OIG system - Kapstone Provide a future phase blueprint with high level tasks and milestones for future phases –Kapstone	– Knowledge Transfer Document (for CCG Admins and end users) - Kapstone – End User Training Document - Kapstone – Postproduction Operational Support - Kapstone	– Kapstone Managed Services teams will maintain and support the OIG Environment. Kapstone will provide troubleshooting support (related to code/configuration issues) for the warranty period. Kapstone’s team will work Cook County’s IT Operations team to review

		– Conduct Lessons Learnt – Joint Ownership	the configuration document, if required. – The post-production support will be executed as per CCG team’s requirement.

6.2.1. CCG Resource Requirements

Detailed CCG resource schedule will be provided upon request or during planning phase.

Staff Needed	Qualifications	Roles/Responsibilities	% of time for each resource
Project Manager	Knowledge of CCG Project Management processes and tools.	Coordinate calls, meetings and communications between Admin, Stakeholders and project team throughout the project implementation phase. Inform project status, schedule and key issues to application stakeholders and management on regular basis. Perform negotiations on project activities with Stakeholders when required.	Recommend a dedicated project manager for the first two years of engagement.
IAM Technical Lead	Knowledge of CCG Identity Management Processes and Understanding of Basic Java Skill	Responsible for managing IAM solution after implementations	30% During Project Kick-off, Discovery and Design. 15-20% during development phase 40% during UAT 80% During Go-Live
System Administrator	Knowledge of CCG AD, Azure, OCI	Responsible hardware setup, backup and Recovery	Depending upon the HA/DR requirement, we will need Sys Admin to setup servers and configure pre-requisites

Application Owners	Business Owner of the Application.	Provide business process flow to manage account and access	Require up to 2 weeks to understand application flow, account management process during the discovery, design and UAT phases based on the need
DBA	Knowledge of OCI and Database	Responsible for Database schema creation, Backup and Recovery	Estimated to require up to 4 weeks to install various Schemas and setup backup and Recovery for each environment. Also responsible for setting up DB replication if HA is desired.
Network Admin		Responsible for Load Balancer, Virtual IP creation, DNS Setup, Firewall Configuration	Time requires to setup load balancer entries, Virtual IP, DNS Entries and Firewall Configuration for various IAM Services
Project Sponsor, Key Stakeholders and CISO		Responsible for Overall IT security Strategy. Provide overall IT security vision of the county. Also explain audit, compliance and reporting requirements.	Participation during monthly and quarterly stakeholder briefing.

6.2.2. Project Deliverables (RACI)

Below is the RACI (R - Responsible, A – Accountable, C – Consulted, I – Informed.) Matrix.

#	Deliverables/Activities	Kapstone	CCG
1	Requirements analysis	A, R	R
2	Functional design	A, R	C
3	Technical design	A, R	R

4	Project plan	A,R	C
5	Design sign-off	C	A,R
6	Install, configure and deploy in all the in-scope environment	A, R, C	A, R
7	Migrate OIM configurations	A,R	I
8	Migrate connectors based on priority and application grouping	A,R	C
9	Migrate data using recon process	A,R	C
10	Configure audit and report	A,R	C
11	Unit testing	A,R	I
12	Iterative flow from 7-11 for remaining application integration	A,R	I
13	Test environment build using T2P	A,R	I
14	System integration testing	A, R, C	A, R
15	SIT and Sign-Off	C	R
16	QA environment build using T2P	A,R	I
17	User acceptance testing / Performance Testing	A, R, C	A, R
18	QA and Sign-Off	A,C	A,R
19	QA Support	A, R	A
20	Code Freeze	A,R	A,R
21	UAT environment build using T2P	A,R	I
22	Performance Testing	A, R, C	A, R
23	UAT and Sign-Off	A,C	A,R
24	UAT Support	A, R	A
25	Production environment build using T2P	A,C	A,R
26	Sanity Testing	A, C	A, R
27	Switch over to Production	A,C	A,R
28	Postproduction Support	A, R	I,R
29	Knowledge Transfer	A, R	I,R
30	End User Training	A, R	I,R
31	Conduct Lessons Learnt	A, R	I,R

7. Support and Maintenance.

7.1. Post-Production Support

Kapstone will provide six weeks of post-production support to stabilize the EIAM environments and to support knowledge transfer activities. The post-production support will be provided primarily by the staff members from the implementation team along with the support personnel from the managed services group. The services provided will include:

- Coordinating with the County's Service Desk to provide Level 2 and Level 3 Support for the EIAM installation and the scoped application integrations.
- Documenting and escalating issues with the project management team as necessary for resolution and deployment.
- Continuing to provide knowledge transfer to County staff as required.
- Monitoring the system and resolving issues.
- Coordinating reporting of product issues to the product vendor support and following up for Oracle & CyberArk vendor patches/solutions and implementing the same as needed.
- Transitioning open issues to the extended support services team at the end of the support period.

The goal of this post-production support is to ensure that the EIAM environments are stable and that the County staff is able to use them effectively. The support team will be available to answer questions, troubleshoot issues, and provide training as needed.

7.2. Managed Support Service

Kapstone will provide Managed Services Support after the post-production support and until the contract period. The support services will include diagnosis and resolution of issues related to the EIAM platform and the application integrations.

Managed services will include the following services –

- Service delivery management
- Transition from the Implementation Team to Managed Services team.
- Troubleshoot and resolve level 2 and 3 issues of EIAM platform or resolve critical and high-priority EIAM related tickets.
- Update and Maintain RAID logs, operational runbook document and perform Minor enhancements.
- Patch critical security and vulnerability issues as agreed to by Kapstone and the County on a case-by-case basis.
- Kapstone will provide the County with regular reports of all available patches and an assessment of the importance of each respective patch to the scope of the project.
- Provide Technical support.

In addition to other items listed in this statement of work (SOW), the following assumptions apply:

- Kapstone will provide remote post-production support services within the continental United States. They will not perform any work outside of the continental United States that involves access to PII, CJIS, HIPAA, or other confidential data.
- Kapstone will provide the County with a list of all personnel who will have remote access to County environments and applications at least semi-annually, or in the event of a termination. This will allow the County to track who has access to its systems and data.

- Kapstone will provide the County with user access review attestation for their employees who have access to County systems at least annually, or upon County request. This will ensure that only authorized personnel have access to the County's systems and data.
- Kapstone will submit access request forms for any new staff to the County for each individual employee requiring access to the system. This will allow the County to approve or deny access to its systems and data on a case-by-case basis.
- Kapstone personnel will monitor critical alerts for the OIAM and PAM System and for the application integrations. This will help to ensure that the County's systems are up and running and that any issues are resolved quickly.
- Kapstone personnel accessing sensitive data will have prior County clearances including required training completion. This will help to ensure that only authorized personnel have access to sensitive data and that they are properly trained on how to handle it.
- All times stated in this document are Central Standard Time (CST) unless otherwise noted. This will help to avoid any confusion about when certain tasks or events are scheduled to occur.
- The support coverage for service requests will be commensurate with the urgency of the issue (incident type). This means that more urgent issues will be given higher priority and will be resolved more quickly.
    - Any development performed by the County or third party engaged by the County will be subject to technical quality testing process and approved by Kapstone (which approval will not be unreasonably withheld, delayed or conditioned) before it can be added as an in-scope application component. This will help to ensure that any new development is of high quality and meets the County's requirements.
    - If Kapstone reasonably believes the addition of such development as an in-scope application development will impact its service delivery and/or fees, Kapstone will raise a change request pursuant to the Change Order process. The new items will not be added to scope until the approval of the associated changer order. This will help to ensure that Kapstone is compensated fairly for any additional work that it is required to do.

The primary scope of the service is the Support, Management and Enhancement of Oracle IAM and PAM including below services:

Account Management / Risk & Quality
Access Management - Federated Applications
Access Management - Webgate applications
External Identity Management
Multi-factor and Adaptive Access Management
Internal Identity Management
Application Onboarding / Integration
Testing
Operational Support (Level 2)
Operational Support (Level 3)

Kapstone will maintain the overall architecture of the system with the following components (as listed below),

Sl No	Component
1	Oracle Identity Manager, Oracle Access Manager, Oracle Unified Directory
2	CyberArk PAM solution
3	Mod Auth Plug-Ins (SAML, OIDC, Shib)
4	Oracle HTTP Proxy Servers, App gateways, Oracle Webgates
5	Custom Login Application
6	OIM Connector Servers
7	OAA, OARM, ORA
8	CloudNuro.ai

The following services are offered as part of the Manage, Operate & Enhance contract.

- **Maintenance Services:** All Maintenance requests will follow through County change management process and Kapstone will align to the processes followed by County and adhere to them.
- **Application QA service:** Kapstone will follow standard documentation on testing changes before they are deployed in Production. The changes will go through Unit testing in development environment and the testers will produce a unit test report approved by the IAM lead. In the Test environment System integration testing is performed to ensure end to end integration cases are achieved. Wherever required Regression test cases will be executed and the final code prepared for deployment to Production.
- **Release Management:** Kapstone will follow standard configuration management processes of ETS to deploy changes to production, Kapstone will appoint a Release Manager as an internal role within the team to co-ordinate the release management objectives. Kapstone will follow naming conventions and code packaging version control to manage and deploy code from DEV->QA-> UAT→PROD.
- **Preventive Maintenance:** Kapstone will use the inbuilt feature of Oracle IAM solutions to monitor the health of the system, Kapstone also has predefined assets to monitor services on windows and Unix / Linux platforms which will check for the system availability and alert via email on the current status of the system, this is in addition to build in capabilities of Oracle IAM product. Patch management systems will follow a quarterly cycle unless a high impact patch is recommended by Oracle IAM Solution. Kapstone will take care of all necessary proactive methods to have the patch to minimize risk to IT systems.
- **Operational Reporting:** Kapstone will provide a weekly report and a forum to discuss the ongoing issues with all support stakeholders and third-party suppliers of County. This will provide higher team interaction and will build a base for proactive maintenance. There will also be a Monthly service Review meeting with the County and Kapstone LLC management to review the status of the SLA's, ongoing issues and escalations.

Exclusions (Out of Scope):

The following are not included in this Statement of Work (SOW):

- Kapstone will work with software vendors on behalf of the County to resolve issues related to in-scope vendor software and hardware. Kapstone will not be responsible for the software or hardware vendors performance or functionality of any solutions, hardware, or cloud infrastructure.

- Any changes and support for target agency applications and HR applications, unless otherwise specified in this SOW.
- Support for County development, maintenance, or problem resolution related to County-owned or leased networks, including but not limited to Local Area Networks (LAN), Wide Area Networks (WAN), leased lines, firewall, server/data backup, data archive, load balancer, DNS, AD, and Exchange, unless otherwise specified in this SOW.
- Support for County development, maintenance, or problem resolution related to County workstation and/or desktop issues, unless otherwise specified in this SOW.
- Support for new developed functionality or new application integrations that are implemented by the County, or a third party engaged by the County.
- Any major upgrade to any product implemented as part of the OIAM and PAM project.
- New product implementation.

Level 1 Support / Service Desk:

The County will be responsible for providing Level 1 Helpdesk/Service Desk support. The primary responsibility of the County Level 1 Helpdesk is to provide a single point of contact for County EIAM end users, gather initial information on Service Incidents and/or Service Requests, resolve Service Incidents that are within their scope of service, and forward unresolved Service Incidents and/or Service Requests to the Kapstone Managed Services support resource.

The County's Level 1 Helpdesk agents will:

- First Point of Contact: County's help desk Act as the initial point of contact for the users seeking technical assistance over the phone or email. Provide general user support, including IAM application usage, often tailored to specific needs (password management, authentication, authorizations, access control) of the end users.
- Ticket Management: Record events and problems and their resolution in logs, often through a ticketing system.
- Guidance: Guide users through step-by-step solutions or set up remote sessions to directly address the issue or escalate if necessary.
- Vendor Coordination: Liaise with Kapstone support team for IAM related tickets and incidents.
- Feedback and Improvement: Collect feedback from users to improve training methods and service delivery.
- Assist in training newer staff members on the helpdesk team.

In addition to these duties, Level 1 Helpdesk agents may also be responsible for other tasks, such as:

- Creating and maintaining knowledge bases and FAQs. Kapstone will provide the knowledge base templates and FAQ document templates.
- Participating in quality assurance and process improvement initiatives
- Attending Kapstone IAM related workshops to stay up-to-date on EIAM application usage

In addition, the County will:

- Provide Kapstone with up-to-date electronic contact lists of their designated personnel, such as help desks within each business area and individuals to be notified in escalation situations.
- Ensure that all County users follow the call flow process.
- Log all incidents through the County's Level 1 ITSM tool.
- Service incidents are related to a single reported problem. Multiple problems grouped into a single service incident are equivalent to multiple service incidents and are tracked accordingly.
- Provide Kapstone access to the Ticket Management System as needed for Kapstone to provide the Services described in this SOW, including an appropriate means of tracking incidents and generating appropriate incident management statistics to enable service level reporting.

7.2.1. Managed Services Tasks and Service Delivery Management:

Ongoing service delivery management will focus on the following:

- Coordinating Kapstone Support personnel, project communications, reporting, procedural activity, and contractual activity.
- Participating in monthly status meetings and preparing status reports.
- Preparing a strategic support plan on an annual basis. The plan will include:
    - A review and assessment of the immediately preceding Annual Plan.
    - A review and assessment of the impact on the Services of the County's operational and IT strategies and plans to the extent made known to Kapstone.
    - A discussion of major EIAM platform maintenance activities undertaken during the previous year and/or any planned future EIAM platform maintenance activities.
    - Review any plans for major maintenance activities planned for the year.

Troubleshoot and Resolve Issues (Level 2 and 3 Support)

The Troubleshoot and Resolve service diagnoses and resolves issues caused by problems with EIAM

Tasks shall include:

- Receive service incidents from the Level 1 helpdesk for service incidents caused specifically by breaks in scoped OIAM and PAM installation and application integrations.
- Work with the County to prioritize the resolution of severity tickets based on established criteria.
- Implement and migrate into the production environment.
- Communicate service incident resolutions through defined processes.
- Resolve security vulnerabilities identified in the System software and Source Code created by Kapstone.
- Update system and user documentation as required.

Kapstone Responsibilities to resolve a service incident.

The following steps will be taken to resolve a service incident:

1. Confirm the initial severity level.
2. Gather the required information to determine the cause of the incident.
3. Diagnose the problem and determine the cause.
4. Adjust the severity level if necessary and approved by the County.
5. Perform root cause analysis for the problem ticket.
6. Perform problem management and escalation in accordance with the call flow process, including escalation to the application software supplier if necessary.
7. Determine viable resolution options.
8. Determine the desired resolution.
9. Apply the desired resolution and/or corrective action to the development system.
10. Unit test the resolution in the development system.
11. Update the relevant system, configuration, or process documentation.
12. Resolve the service incident or effectively transfer the service incident to the appropriate area of support.
13. Document and promptly notify the County of any emergency changes per County SLAs.
14. Apply the solution into the production environment.
15. Work with the third-party software maintenance vendor in case of software defects

The County (CCG) responsibilities to resolve a service incident.

1. Make sure that users report service incidents through the agreed-upon call flow process. - This means that users will report service incidents through the designated channels, such as the help desk or a ticketing system. This will help to ensure that incidents are reported in a timely manner and that they are routed to the appropriate people for resolution.
2. Assign severity levels to tickets according to the agreed-upon criteria.
3. The severity level of a ticket will be assigned based on the impact of the incident on users. For example, a ticket that affects all users of a service will be assigned a higher severity level than a ticket that affects only a small number of users.
4. Provide SME support for issue resolution - SME support can be provided by subject matter experts (SMEs) who have specialized knowledge of the service or technology that is affected by the incident. SMEs can help to troubleshoot the issue and identify the root cause.
5. Perform UAT after the issue has been resolved - UAT, or user acceptance testing, is a process that is used to verify that the issue has been resolved and that the service is working as expected. UAT will be performed by users who are familiar with the service.
6. Sign off on migration to production - Once the issue has been resolved and UAT has been completed, the service can be migrated to production. This means that the service can be made available to all users.

7.2.2. Enhancements Approach

Kapstone is offering an annual support allocation of up to 480 hours specifically dedicated to minor improvements in the existing OIAM and PAM environment. Minor improvements refer to discrete tasks, each requiring less than 40 hours for completion. These tasks encompass a range of activities, such as modifications to scoped application integrations and the addition of new features. It's important to note that this service is an optional addition and will be undertaken only if there are surplus hours available once Break/Fix and system maintenance activities have been fulfilled. All enhancement requests must receive written approval from the designated County Coordinator responsible for production support. Work will commence only after Kapstone, and the County have mutually agreed upon written estimates for the proposed tasks.

Kapstone Responsibilities

- Receive service requests initiated through the Service Request process.
- Evaluate service requests and generate cost estimates for each submitted request.
- Design, create, or modify code or configurations in accordance with the approved design.
- Implement the code in the production environment following the BOT's Change Management process.

County Responsibilities

- Authorize the submission of all tasks delegated to Kapstone.
- Specify prerequisites using a Service Request.
- Formulate and create user test scenarios and test cases.
- Assist with integration testing and execute user acceptance testing.
- Grant approval for the closure of the service request.

7.2.3. Technical Support

Kapstone responsibilities include identifying vendor-mandated patches, fixes, and updates that require analysis, in this case, product vendor-related. Kapstone will collaborate with the County to assess the necessity of applying these patches, fixes, and updates to the County Application Environment. If the County decides to proceed with the application of these patches, fixes, and updates, Kapstone will work closely with the County to manage their installation.

Following installation, Kapstone will conduct testing on these patches, fixes, and updates and will coordinate the User Acceptance Test in conjunction with the County. After these items have been successfully tested in alignment with the County's testing strategy and have received County approval, Kapstone will execute the migration of the patches, fixes, and updates to the Production environment.

7.2.4. EIAM Software Infrastructure Support

7.3.

Kapstone shall provide support for maintenance of the Oracle IAM and CyberArk PAM software infrastructure to assist in providing high level of system availability. The following are the high-level tasks:

- Provide support in diagnosing system issues related to the County's OIAM and PAM environment.
- Work with Oracle and CyberArk product support in troubleshooting and identifying platform problems.

- Execute a backup and recovery strategy to enable either point-in-time recovery or version recovery, as directed by the County.
- Apply necessary fixes, updates, and patches to address platform issues.
- Carry out any necessary pruning, rotation, or archiving of application and database log files.
- Conduct reporting and assess compliance findings as needed.
- Keep user and system documentation, as well as security and compliance documents, up to date as required.

County Responsibilities

Manage an Oracle IAM software and PAM maintenance contract throughout the duration of this agreement. Give the ultimate approval for the selection of patches, fixes, and updates to be applied and determine their timing, taking into consideration other ongoing initiatives.

7.3.1. Incident Types

Requests for assistance are categorized within five support levels:

- Critical/Urgent – Refers to tasks demanding immediate support due to incidents that disrupt critical business functions, causing a complete or significant halt in operations with no available workarounds.
- High Priority – Encompasses incidents where the system/application functions with severe limitations, such as unacceptable performance degradation.
- Medium Priority – Pertains to production system/application issues where acceptable workarounds are available. Most functions remain operational, although some temporary measures may be needed to restore normal service.
- Low Priority – Involves production system/application issues that impact only a limited number of individuals and/or non-critical tasks.
- Regular Incidents – Encompasses routine monitoring and support activities for the County's OIAM and PAM environment.

7.3.2. Support Hours

Except for the critical issues or high severity issues, EIAM support will be provided during normal business hours as below:

8:00 AM to 5:00PM CST Monday-Friday (expect public holidays)

Emails containing support requests, except for critical matters, that are received after regular business hours or during weekends will be assessed on the following business day, and the response will be determined based on the priority hierarchy mentioned above. For critical issues, as defined in the "Service Level Agreement - Response Times" section, efforts will be ongoing until resolution or a priority change occurs.

7.3.3. Service Level Agreement - Response Times

Table: SLAs Response Times

Severity	Response Time	Comments

P1 - Critical	1 Hour	Begin analysis and Communicate once very 2 hours until resolved or severity changes
P2 - High	4 Hours	Begin analysis and work on these within 8 hours and continue to work on this until the issue is resolved or the priority changes.
P3 - Medium	8 hours	Begin analysis and work on these within 2 business days
P4 - Low	2 Business Days	Communicate confirmation of scope and impact of incident within 5 business days of initial contact
P5 – Normal / Regular Maintenance		

Table: The detail severity and action details

Priority	Actions
Critical	• Acknowledgment via telephone or email within 60 minutes of notification. • Provide confirmation of the incident's scope and impact within 120 minutes of the initial contact. • Allocate resources to address the issue within 2 business hours. • If needed, create a Service Request (SR) with Oracle. • Update on progress and outcomes at least once every 120 minutes until the matter is resolved or the priority is altered. • For all Critical Break Fix issues, immediate escalation to the County Support Manager is mandatory. • Ensure that resources are assigned and available around the clock to work on the incident until it is resolve
High	• Confirmation will be provided via phone or email within four hours during regular business hours. • Within eight hours of the initial contact, we will relay the confirmation of the incident's scope and impact. • Initiate analysis and commence work on these matters within eight hours, persisting until the issue is resolved or priority adjustments are made. • If required, create a Service Request (SR) with Oracle or software vendor and document it. • Report on progress and outcomes every business day until resolution or a change in priority.
Medium	• Confirmation will be made via telephone or email within 8 hours during regular business hours. • Commence analysis and start work within 2 business days. • Relay confirmation of the incident's scope and impact within 4 business days of the initial contact. • Create a Service Request (SR) with Oracle, if it becomes necessary. • Provide updates on efforts and outcomes once every week until the issue is resolved or there's a change in priority.
Low	• Acknowledgment will be made via telephone or email within 2 business days. • Initiate analysis and provide work estimates for these items within 5 business days. • Share confirmation of the incident's scope and impact within 5 business days of the initial contact. • If required, create a Service Request (SR) with Oracle. • Share progress updates and results on a weekly basis until the issue is resolved or there's a change in priority.
Regular Maintenance	• Work will be conducted within standard business hours. • Scheduled production migration will take place outside of business hours or on weekends. • Necessary communication will be furnished to the County Support Manager.

7.3.4. Optional Services (Not Scoped)

The County reserves the right to decide whether to enlist Kapstone for the following supplementary, non-exclusive services, which are presently not detailed in the scope:

- Creating new application onboarding procedures and/or improving existing application integrations.

- Extending production support to systems and applications beyond the currently defined services.
- Offering additional services related to Identity governance, PAM (Privileged Access Management), security, single sign-on, and other technological initiatives.

Any additional scope will be addressed through the SOW (Statement of Work) Change Order process.

7.3.5. Project Assumptions

- Oracle, as the provider of Licensed Software, will be solely responsible for the compliance with any Licensed Software-specific RFP requirements, including, but not limited to, Software Maintenance and Technical Support, Licensed Software Documentation, and any other terms and conditions to the extent they apply to such Licensed Software, including the CCG Data Safeguard Standards and Accessibility requirements.
- Oracle E-business Suite is the authoritative source of user identities for CCG.
- CCG will be responsible for any application configuration changes which may be necessary to integrate with the new IAM solution.
- Necessary stakeholders will be available to review and approve the proposed design.
- CCG will have dedicated Project Managers and Release Managers to coordinate releases and activities.
- There will be a max of five Environments in scope: Development, Test, UAT, DR and Production. The following user populations are in scope: employees and contractors.
- Kapstone is not responsible for data quality issues initiated from dependent or definitive targets and/or any applications feeding the CCG during identity transaction processing. CCG is responsible for data cleansing, validation of user stores.
- CCG is responsible for driving priority among the application portfolio owners; Kapstone is not responsible for delays reasonably attributable to CCG's resources or applications owners.
- CCG is responsible for change management planning and execution during this engagement. Managed operations of the existing IAM platform are not in scope for this proposal.
- Holiday and environment freeze periods may impact delivery dates estimated in this document.
- Decisions to be made by CCG will be made promptly and without undue delay, but in no event later than ten(10) business days from the time the request is made (unless otherwise mutually agreed by the parties). Kapstone and CCG will collaborate to raise issues in a timely fashion and will coordinate during the Project Steering Committee Meetings.
- CCG will provide the necessary documentation (Requirements, Technical and Logical design, Network architecture, etc.) for existing implementations.
- Key CCG resources will be available for information clarification, review and to provide sign off as needed.
- Availability of the applications for integration in the various deployment environments as per the planned timelines for integration
- The business requirement will be re-evaluated at the beginning of each phase considering Oracle product roadmap and maturity. E.g., application on-boarding in OIAM 12c might not provide all the capabilities of maintenance tool.

8. Key Personnel.

Below are the key designated resources from Kapstone for this project.

RESOURCE	PROJECT ROLE	Relevant IAM Experience
Shyam Kumar	Program Manager	20+ Years
Nayan Baid or Tushar Jagadale	IAM Solution Architect	15+ Years
Harish Jangada	Engagement Executive and Subject Matter Advisor	25+ Years

9. Payment and Pricing.

This section lists the details of pricing and payment schedule for Enterprise IAM Project. Invoices must conform to the terms set forth in Article 5, Section (b) of the Exhibit VI - Professional Services Agreement. Kapstone travel expenses are incorporated into pricing for implementation services, managed services and all other services under this Agreement, except as set forth in Sections 9.4 Additional Service and 9.5 Optional Fees. The start date or dates below are contingent on approval of the County Board.

9.1. Software Fee

Below is the list and pricing of additional software for Enterprise IAM implementation in the County.

Table 9.1: Software Fee

ID	Software Functionality	Module Name	Annual Cost	5 Year Cost
3.001	Oracle Cloud Infrastructure (OCI) - Government Cloud*	OCI and Oracle PaaS Components	$ 200,000	$ 1,000,000
3.002	CloudNuro Platform - Managed IaaS, PaaS, SaaS	Managed Services for Cloud/SaaS	$ 30,000	$ 150,000
3.003	CyberArk Software - PAM	Privileged Standard User SaaS	$ 75,000	$ 375,000
Total Software Fee (5 Yrs)				**$1,525,000**

**NOTE – OCI cost is the best estimated cost which may vary depending upon the consumption on OCI.*

Table 9.1.1: Payment Schedule by Milestone

ID	Software Functionality	Annual Cost	Est. Due Date
3.001.1	Oracle Cloud Infrastructure - Government Cloud	$ 200,000	03/04/2024
3.001.1	CloudNuro.ai Platform - Managed IaaS, PaaS, SaaS	$ 30,000	03/04/2024
3.001.1	CyberArk Software - PAM	$ 75,000	03/04/2024
Total Software Fee (Year One)		**$ 305,000**	

9.2. Deliverables Fee

The County shall pay for implementation services by Deliverable. Upon the County's Acceptance of any Deliverable or Milestone set forth in Table 9.2, Kapstone will submit an invoice to the County in the amount of the Deliverable.

The following is the implementation of the Services Payment Schedule for Deliverables.

Table 9.2: Deliverable Payment Schedule by Milestone

Year 1 (Enterprise IAM Platform)				
#	**Deliverable**	**Phase**	**Cost Per Deliverable**	**Milestone Completion Dates***
4.003	Project Charter	1	$ 199,500	3/15/2024
4.004	Project Plan Approved	1	$ 95,000	4/13/2024
4.005	Requirement Specification Created	1	$ 399,000	6/15/2024

4.006	Infrastructure Design Completed	1	$ 199,500	6/19/2024
4.007	Technical Design Completed	1	$ 399,000	7/20/2024
4.008	Dev Env Created	2	$ 104,500	8/17/2024
4.009	QA Env Created	2	$ 199,500	9/18/2024
4.010	Test Strategy and Plan Created	2	$ 199,500	10/5/2024
4.011	Test Cases Developed	2	$ 104,500	10/19/2024
4.012	System Testing Completed	2	$ 95,000	11/16/2024
4.013	UAT Completed	2	$ 104,500	12/7/2024
4.014	PROD Environment Created	2	$ 256,500	12/21/2024
4.015	Production Go-Live	2	$ 237,500	1/4/2025
4.016	DR Environment Completed	2	$ 98,373	1/4/2025
Year 2 (Agency, Application On-boarding)				
	Iteration 1			
4.018	Dev Env Updated	3	$ 85,500	2/25/2025
4.019	Test Env Updated	3	$ 85,500	3/25/2025
4.020	SIT Completed	3	$ 85,500	4/9/2025
4.021	UAT Completed	3	$ 85,500	4/24/2025
4.022	Production Go-Live	3	$ 85,500	5/24/2025
	Iteration 2			
4.022	Dev Env Updated	3	$ 85,500	5/24/2025
4.023	Test Env Updated	3	$ 85,500	6/21/2025
4.024	SIT Completed	3	$ 85,500	7/5/2025
4.025	UAT Completed	3	$ 85,500	7/19/2025
4.026	Production Go-Live	3	$ 85,500	8/16/2025
	Iteration 3			
4.027	Dev Env Updated	3	$ 76,000	8/19/2025
4.028	Test Env Updated	3	$ 76,000	9/16/2025
4.029	SIT Completed	3	$ 76,000	10/1/2025
4.030	UAT Completed	3	$ 76,000	10/16/2025
4.031	Production Go-Live	3	$ 76,000	11/15/2025
	Iteration 4			
4.032	Dev Env Updated	3	$ 23,750	11/15/2025
4.033	Test Env Updated	3	$ 56,344	12/13/2025
4.034	SIT Completed	3	$ 71,250	12/27/2025
4.035	UAT Completed	3	$ 71,250	1/10/2026
4.036	Production Go-Live	3	$ 71,250	2/7/2026
4.037	Support Transition Completed	3	$ 71,250	3/7/2026
Total IAM Implementation Project Cost			**$ 4,291,967**	

*NOTE – Milestone dates will be finalized during the project initiation phase in consultation with the County Project Manager.

9.3. Managed Support Services Fees

The extended production support services included in the scope for five years (60 months). It may be optionally extended for two one-year terms for a fee of $600,000/year.

Table 9.3: Payment Schedule by Milestone

#	Item	Total Cost	Milestone Completion Dates *
5.002	Managed Support for IAM - Support Year 1	$ 0	
5.003	Managed Support for IAM - Support Year 2	$ 540,000	03/04/2025
5.004	Managed Support for IAM - Support Year 3	$ 540,000	03/04/2026
5.005	Managed Support for IAM - Support Year 4	$ 540,000	03/04/2027
5.006	Managed Support for IAM - Support Year 5	$ 540,000	03/04/2028
Support and Maintenance Total		**$ 2,160,000**	

9.4. Additional Services Fees

Included as part of the cost schedule, the County will have a discretionary bucket of one thousand (3,000) hours for use toward any additional out-of-scope work. No work shall be performed against these hours without written approval from the County's designated project manager. The County shall apply Kapstone's rate card listed in Section 9.8 to determine the fees for the additional work. The total amount of additional services fees shall not exceed $540,000.

9.5. Optional Services Fees

CISCO ISE resource allocation and CyberArk PAM professional services cost allocation is in below table.

Table 9.5: Payment Schedule by Milestone

	Optional Deliverable	Insert RFP Project Sections	Cost Per Deliverable	Milestone Completion Dates *
6.003	CyberArk - PAM	CyberArk Professional Services	$ 300,000	Table 9.5.1
6.004	Cisco ISE	1.5 FTE resource budgeted with hourly rate $150 for 18 months*	$ 864,000	TBD
	Optional Services Total Fee		**$ 1,164,000**	

NOTE - Additional clarifications required from County on the Scope of work, and Engagement Dates during the project kickoff.

Table 9.5.1: Payment Schedule by Milestone – CyberArk Professional Services

	Optional Deliverable	Cost Per Deliverable	Milestone Completion Dates *
6.003.1	CyberArk Professional Services - Requirement	$ 75,000	2/25/2025
6.003.2	CyberArk Professional Services - Design	$ 75,000	5/24/2025
6.003.3	CyberArk Professional Services – UAT	$ 75,000	8/19/2025
6.003.3	CyberArk Professional Services – Go-Live	$ 75,000	11/15/2025

	CyberArk Professional Services Total	$ 300,000	

9.6. Pricing Summary

Listed below is the pricing summary.

Table 9.6: Pricing Summary

#	Item	Total Fees
1	Hardware Fee	**$0**
2	Software Subscription (5 Years)	**$1,525,000**
3	Deliverables Fee (Implementation Services)	**$4,291,967**
4	Managed Support Services (5 Years)	**$2,160,000**
5	Optional Services Fee	**$1,164,000**
6	Additional Services - 3,000 hours	**$540,000**
	Total Fee (Summary)	**$9,680,967**

9.7. Estimated Payment Schedule by Fiscal Year

The following is the estimated payments by Fiscal Year:

Table 9.6.1: Payment Schedules by Fiscal Year

Item	**FY-2024**	**FY-2025**	**FY-2026**	**FY-2027**	**FY-2028**	**Total**
	12/1/23 to 11/30/24	**12/1/14 to 11/30/25**	**12/1/25 to 11/30/26**	**12/1/26 to 11/30/27**	**12/1/27 to 11/30/28**	
Hardware	$0	$0	$0	$0	$0	**$0**
Software Subscription (5 Years) Fee	$305,000	$305,000	$305,000	$305,000	$305,000	**$1,525,000**
Deliverables Fee (Implementation)	$1,995,000	$1,955,623	$341,345	$0	$0	**$4,291,967**
Managed Support Services (5 Years)	$0	$ 540,000	$ 540,000	$ 540,000	$ 540,000	**$2,160,000**
Optional Services Fee	$432,000	$532,000	$200,000	$0	$0	**$1,164,000**
Additional Services - 3,000 hours	$90,000	$180,000	$90,000	$90,000	$90,000	**$540,000**
Total by Financial Year	**$2,822,000**	**$3,512,623**	**$1,476,345**	**$935,000**	**$935,000**	**$9,680,967**

9.8. Rate Card

Below hourly labor rate card will be applied for any additional services. No work shall be performed without a written approval from the County. The hourly and travel rates will increase annually at CPI+2%

Table 9.8: Hourly Rate Card

#	Role	Hourly Rate
4.002	Project Manager	$200
4.003	IAM Solutions Architect	$225
4.004	IAM Architect (IDM/SSO)	$200
4.004b	IAM Developer 2 (IDM/SSO/UI)	$180
4.005	IAM Developer 3 (IDM / SSO /PAM / Java)	$180
4.006	IAM Developer 4 (BI / DB / IAM / PAM)	$180
4.007	Business Analyst	$165
4.008	DevOps Engineer & DBA	$165
4.009	QA Lead	$165
4.010	Cisco ISE	$150

Appendix – A (Definition and Acronym)

Kapstone has submitted the updated contract agreement.

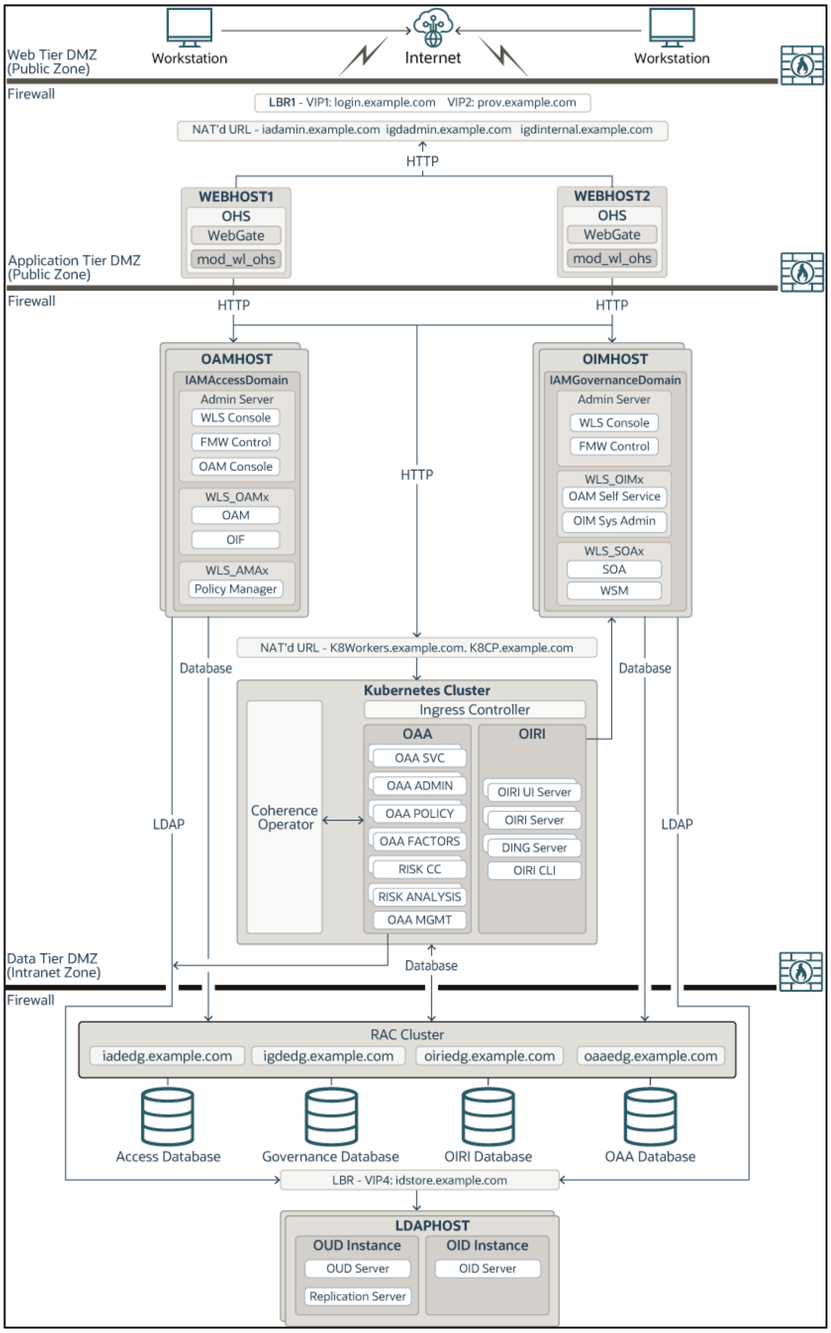
Acronym	Explanation
IAM	Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.
IDM	Identity management (IdM) is a set of practices that help manage user identities within an organization.
OIM	Oracle Identity Manager enables organizations to effectively manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall and into the cloud.
K8	Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services. Oracle Identity Manager 12c can be set up on containers using Kubernetes.
MSP	Managed Service Provider is a company that offers a computing framework platform for organizations to on-premises or remotely manage a customer's IT infrastructure.
RFP	Request for Proposal is a document that solicits proposal, often made through a bidding process, by an agency or company interested in procurement of a commodity, service, or asset, to potential suppliers to submit business proposals.
OIG	Oracle Identity Governance enables organizations to effectively manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall and into the cloud.
SOW	Statement of Work is document routinely employed in the field of project management. It is the narrative description of a project's work requirement. [1] It defines project-specific activities, deliverables and timelines for a vendor providing services to the client.
SI	System Integrator is a partner that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together. Kapstone will be system integrator in the current OIM Implementation RFP context.
IDCS	Oracle Identity Cloud Service is the next generation comprehensive security and identity platform that is cloud-native and designed to be an integral part of the enterprise security fabric, providing modern identity for modern applications. CCG is using Oracle IDCS along with few Oracle cloud applications.
RBAC	Role Based Access Control is a method of restricting Enterprise application access based on the roles of individual users within an enterprise. Roles can be defined based the job code, department, location information of users.
REST	Representational State Transfer is a software architectural style that defines a set of constraints to be used for creating Web services. OIM provides REST interface to integrate with enterprise applications to provision account and accesses or to manage information in OIM.
API	Application Program Interface is a set of routines, protocols, and tools for building software applications.
DevOps	Development and Operations is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support. Few primary practice areas that are usually discussed in context of DevOps. • **Infrastructure Automation** – create CCG's systems, OS configs, and app deployments as code. • **Continuous Delivery** – build, test, and deploy CCG's apps in a fast and automated manner. • **Site Reliability Engineering** – operate CCG's systems; monitoring and

	orchestration, sure, but also designing for operability in the first place. Kapstone will collaborate with CCG engineering team to enable DevOps capabilities on EIAM environment.
PMI	Project Management Institute is a global nonprofit professional organization for project management
KM	Knowledge Management is the process of capturing, distributing, and effectively using knowledge. KapStone team will work with CCG'S OIM Engineering, OIM Development, OIM operations or support team to transfer the critical business, process and technical knowledge.
TLS	Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network
SOA	Service Oriented Architecture is a software development model that allows services to communicate across different platforms and languages to form applications
AD	Active Directory is Microsoft technology used to manage computers and other devices on a network.
OOTB	Out of the Box refers to a feature or function that are readily available or with minimum configuration in the OIM solution
RTO	Recovery Time Objective is the maximum length of time after an outage that a company is willing to wait for the recovery process to finish.
RPO	Recovery Point Objective is the maximum amount of data loss a company is willing to accept as measured in time.
RPA	Robotic Process Automation is the technology that allows anyone today to configure computer software, or a "robot" to emulate and integrate the actions of a human interacting within digital systems to execute a business process. RPA integration with OIM provide a low-risk, low-cost and low-complexity solution that can be integrated with business quickly and start delivering a return on investment.
DB	Database is an organized collection of structured information, or data, typically stored electronically in a computer system .
CDB	Container Database is the Oracle Multitenant option introduced in Oracle Database 12c that helps to consolidate databases into a standardized database version that is deployed on a shared cloud infrastructure. The option is supported by an architecture in which a host database called the *container database* (CDB) can hold multiple *pluggable databases* (PDBs).
PDB	Pluggable Database is also called as Container Database.
CLI	Command Line Interface is a command line program that accepts text input to execute operating system functions.
IDAM	Identity and Access Management is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.
SDLC	Software Development Life Cycle is a methodology with clearly defined processes for creating high-quality software or solutions.
QA	Quality Assurance is the process of auditing and analyzing the systems which produce a product to improve their quality.
UAT	User Acceptance Testing is a process that confirms that the output of a project meets the business needs and requirements.
SCIM	System for Cross-domain Identity Management is a standard for automating the exchange of user identity information between identity domains, or IT systems.
SoD	Segregation of Duties is a system of internal controls within an organization designed to prevent error and fraud by ensuring that at least two individuals are responsible for the for the separate parts of any task.
Fault-tolerant	Is the capability of a computer system, electronic system or network to deliver uninterrupted service, despite one or more of its components failing.

Scalable	Is the ability of a computer application or product (hardware or software) to continue to function well as it (or its context) is changed in size or volume to meet a user need.
Open Standards	Is a standard that is publicly available, widely adapted by various software vendors and provide vendor neutrality. Many specifications that are not open standards are proprietary and only available under restrictive contract terms. Examples of Open Standards are SCIM, SAML.
IGA	Identity Governance and Administration Services is policy-based centralized orchestration of user identity management and access control that helps support enterprise IT security and regulatory compliance.
Bundle Patch	An official Oracle patch for an Oracle product. Each bundle patch includes the libraries and files that have been rebuilt to implement one or more fixes. All the fixes in the bundle patch have been tested and are certified to work with one another. Regression testing has also been performed to ensure backward compatibility with all Oracle Mobile Security Suite components in the bundle patch.
Our, we, Kapstone	Refers to Kapstone LLC.
You, your, CCG	Refers to Cook County Government Service Corporation for itself and as agent for its affiliated companies of the Cook County Government System.
COE	Center of Excellence
COP	Community of Practice (CoP) is a special type of informal network that shares knowledge and collaborate on social platform or meetups.

Appendix – B (Reference Architecture)

Please see below the reference Deployment of Oracle Identity and Access Management with Microservices (in a Kubernetes Cluster).



Kapstone worked with Oracle Product management team in deploying Oracle PM recommended cloud native technology-based architecture at various customers.

Appendix – C (Additional Design Considerations)

- Enterprise applications which are systems of truth for critical attributes on the user base profile, will be integrated with central master instance and synched with dependent applications.
- For all Citizens facing applications, County agencies with independently elected officials, would participate in the Central framework. Agencies may have local applications, facilities and other resources that would require the agencies continue to have their managed AD forest. Agencies would continue to have their own AD forest for user credentials. To align with central HCM processes, agencies would extend and integrate their employee on/off boarding processes with central county installation. Currently, agencies are collaborating with Central federation engine, which provides one user credential for [Agency] citizen services.
- Citizen Common Profile – One ID - Citizen registration credentials are stored into Citizen AD forest and are synched with Master Credential store for User Discovery, Application attribute management and User profile management. Solution will have a common central trusted application for Citizen user profile registration and account management. Identity federation server landing page will present County/Agency provided services enabled for this One County Access platform, and access to Citizen registration application for profile management.
- Privileged access management solutions will provide privileged account discovery, controlled and audited access, automation, reporting and alert capability for the privileged access related operations.
- Solution will centrally managed policy studio that would define enterprise wide and agency specific policies and that provides traceability for policy enforcement into specific business process implementation.

EXHIBIT 2

SaaS Services Agreement

- CloudNuro Corp agreement attached.
- Oracle and CyberArk – County will use the existing agreements (NASPO or others) with Carahsoft Technology Corporation.

1026 N Cardinal Dr.
Palatine, IL 60074

CLOUDNURO CORP

SAAS SERVICES AGREEMENT

THESE SERVICE TERMS ARE INCORPORATED BY REFERENCE INTO THE ORDER SCHEDULE AND/OR STATEMENT OF WORK EXECUTED BY THE COMPANY IDENTIFIED AS THE "CUSTOMER" THEREIN ("CUSTOMER") AND CLOUDNURO RELLING PARTNER THEREIN ("RESELLING PARTNER" or "SUPPLIER""), PURSUANT TO WHICH THE CUSTOMER RECEIVED THE RIGHT TO USE A CLOUDNURO SUBSCRIPTION SERVICE SUBJECT TO THESE SERVICE TERMS. THESE TERMS MAY NOT BE AMENDED WITHOUT THE WRITTEN CONSENT OF RESELLING PARTNER AND COOK COUNTY'S CHIEF PROCUREMENT OFFICER. THESE TERMS, THE SCHEDULE(S) OR SOW(S) TOGETHER FORM A BINDING AND EXECUTED WRITTEN AGREEMENT BETWEEN CUSTOMER AND SUPPLIER, EFFECTIVE AS OF THE EFFECTIVE DATE OF THE ORDER SCHEDULE (THIS "SAAS AGREEMENT").

1. Service.

(a) Access and Use. Subject to Customer's full and ongoing compliance with the terms and conditions of this SAAS Agreement, Supplier will make the software-as-a-service platform described on the Order Form (the "Service") available to Customer's employees and contractors ("Users") during the Term. Supplier grants to Customer a non-exclusive, non-transferable, non-sublicensable right to permit Customer's Users to access and use the Service in accordance with the terms of this SAAS Agreement. Customer shall remain responsible for each User's access and use of the Service as if such access or use were Customer's own.

(b) Service Guidelines. Except as expressly permitted hereunder, Customer shall not, and shall not permit any User or other third party to (i) interfere with the performance of the Service or the data contained therein; (ii) attempt to gain unauthorized access to the Service or the networks or systems related to the Service; (iii) interfere with another's use of the Service; (iv) permit access to the Service by any third party; (v) use the Service or provide the Service to third parties in any service-bureau or similar capacity; (vi) modify, copy, or make derivative works based on the Service; (vii) disassemble, reverse engineer, or decompile the Service or any software applications associated with the Service; (viii) access the Service to build a competitive service or reproduce features of the Service; or (ix) disclose any User IDs, passwords, tokens, keys or other similar access credentials to the Service.

(c) Customer Content. Customer hereby grants to CloudNuro a worldwide, irrevocable, nonexclusive, non-transferable right to use, host, display, distribute and modify any content provided by or on behalf of Customer or its Users to CloudNuro ("Customer Content") to: (i) provide the Services and perform its obligations under this SAAS Agreement; (ii) to improve CloudNuro's products and services; and (iii) to generate SaaS Usage Data. Customer warrants that it has secured all of the necessary rights for Customer to provide the Customer Content to CloudNuro and for CloudNuro to exercise the foregoing rights in order to provide the Services. Customer acknowledges that Customer Content does not include any aggregated, non-personally-identifiable data or other routines generated by CloudNuro through any automated data analysis, processing or other normal operations of the Service (collectively, "Usage Data"). For the avoidance of doubt, as between the Parties, CloudNuro owns all Usage Data and may use Usage Data without restriction. CloudNuro may remove or restrict access to Customer Content, including if CloudNuro believes such data may violate applicable law, if the source of such data becomes unavailable, or if a third party brings or threatens legal action against Company or a third party

2. Reservation of Rights. Except for the limited rights expressly granted above, as between Supplier and Customer, CloudNuro owns and retains all rights, title and interest, including all intellectual property rights, in and to all technology, software, algorithms, user interfaces, trade secrets, techniques, designs, inventions, works of authorship and other tangible and intangible material and information pertaining to the Service (collectively, "CloudNuro Corp"). All rights not expressly granted hereunder are reserved to CloudNuro.

3. Customer Support. During the term of this SAAS Agreement, CloudNuro will provide to Customer its standard email (support@cloudnuro.com).

4. Confidentiality.

(a) Confidential Information. As used herein, "Confidential Information" means all information of a Party ("Disclosing Party") disclosed to the other Party ("Receiving Party") in connection with this SAAS Agreement.. Confidential Information shall not include any information that: (i) is disclosed by Customer pursuant to the Freedom of Information Act (5 ILCS 140/1, et. seq.) (ii) was already known by the Receiving Party prior to disclosure; (iii) is or becomes publicly available through no fault of the Receiving Party; (iv) is rightfully received from a third party without a duty of confidentiality; or (v) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

(b) Non-Use and Non-Disclosure. The Receiving Party shall not (i) use any Confidential Information of the Disclosing Party for any purpose other than to perform its obligations under this SAAS Agreement, or (ii) disclose Confidential Information of the Disclosing

Party to anyone other than its personnel (including employees, contractors, and consultants) who have a need to know the Confidential Information for the purposes set forth in this SAAS Agreement and who are bound by a written agreement that prohibits unauthorized disclosure or use of Confidential Information that is at least as protective of the Confidential Information as the Receiving Party's obligations hereunder. In no event shall either Party exercise less than reasonable care in protecting such Confidential Information. Notwithstanding the foregoing, the Receiving Party may disclose Confidential Information of the Disclosing Party solely to the extent required by law, provided that the Receiving Party shall make reasonable efforts to provide the Disclosing Party with prior written notice of such compelled disclosure and reasonable assistance (at Disclosing Party's expense) if the Disclosing Party wishes to obtain protective treatment of the Confidential Information.

5. Feedback. Customer may, but is not obligated to, provide CloudNuro with information, suggestions, or other feedback with respect to the Service or CloudNuro Corp ("Feedback"). Customer hereby grants to CloudNuro a worldwide, nonexclusive, perpetual, irrevocable, transferable, royalty-free, fully paid-up, sublicensable license to use and exploit such Feedback for any purpose without restriction.

6. Representations and Warranties.

(a) Mutual. Each Party represents and warrants to the other Party that it has all necessary power and authority to enter into this SAAS Agreement and to carry out its obligations hereunder, and that the execution and performance of this SAAS Agreement does not and will not conflict with or violate any law or its contractual or other obligations to any third party.

(b) CloudNuro. Supplier represents and warrants that it will provide the Service in a professional manner, consistent with applicable law and industry standards.

(c) Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES CONTAINED IN THIS AGREEMENT, THE SERVICE IS PROVIDED "AS IS", AND WITHOUT WARRANTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDNURO HEREBY DISCLAIMS ALL OTHER WARRANTIES UNDER OR IN CONNECTION WITH THIS SAAS AGREEMENT, THE SERVICE, AND ALL CONTENT, INFORMATION, AND MATERIALS PROVIDED THEREWITH, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, SATISFTACTORY QUALITY, TITLE, SECURITY OR INTEGRITY OF DATA, FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE SERVICES WILL BE ERROR-FREE OR UNINTERRUPTED.

7. Indemnification.

(a) By CloudNuro. Supplier will(a) defend (or pay for the defense of), or at its option (with consent of Customer) settle, any claim brought against Customer by a third party to the extent it alleges that Customer's use (as authorized in this SAAS Agreement) of a Service during the Term constitutes an infringement of any intellectual property or proprietary rights of any third party (a "Claim"), and (b) pay any damages awarded in a final judgment (or amounts agreed in a monetary settlement) in any such Claim defended by Supplier; provided that Customer provides Supplier (i) prompt written notice of, (ii) the opportunity to participate in the defense and settlement of, and (iii) all information and assistance reasonably requested by Supplier in connection with the defense or settlement of, any such Claim.

(b) Additional Rights. If any such Claim is brought or threatened, Supplier will, at its sole option and expense: (w) procure for Customer the right to continue to use the applicable Service; (x) modify the Service to make it non-infringing; (y) replace the affected aspect of the Service with non-infringing technology having substantially similar capabilities; or (z) if none of the foregoing is commercially practicable, terminate the Order Form related to the applicable Service or this Agreement and provide Customer with a pro-rated refund of pre-paid fees within 30 days of the Claim being brought or threatened.

(c) Limitations. Notwithstanding the foregoing, Supplier will have no liability to Customer (1) for any use of the Services in combination with software, products or services not provided or recommended by CloudNuro; to the extent that the Services would not be infringing but for such combination or modification; (2) for Customer's material failure to use the Services in accordance with this Agreement; or (3) for any claims related to Customer Content.

8. Intentionally Omitted

9. Term and Termination.

(a) Term. The term of this SAAS Agreement shall begin on the Effective Date and, unless terminated earlier as described below, shall continue for the Subscription Term forth in the Order Form(the "Initial Term").

(b) Termination. Either party may terminate this SAAS Agreement or any Order Form by written notice if the other party is in material breach of this SAAS Agreement or such Order Form, where such material breach is not cured within 30 days after written notice of such breach from the non-breaching party. If Customer fails to pay within 30 days after written notice of nonpayment of any undisputed amounts owed to Supplier, such nonpayment will be deemed a material breach.

(c) Effect of Termination. Upon the effective date of expiration or termination of this SAAS Agreement for any reason: (a) all outstanding Order Forms and access to the Service will automatically terminate Survival. The following provisions will survive any expiration or termination of the SAAS Agreement: Sections, 2, -9, 10(d).

10. Miscellaneous.

(a) Changes. CloudNuro may make changes or updates to the Service during the Term, including to reflect changes in technology, industry practices, patterns of system use, and availability of third-party content. Such changes will not result in a reduction in the functionality or performance of the applicable Service. CloudNuro shall notify Customer of proposed changes or updates and provide Customer with the opportunity to object at least 15 days prior to change or update implementation.

(b) Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable, such provision shall be modified so as best to accomplish the original intent of the Parties, and the remaining provisions of this Agreement shall remain in effect.

(c) Publicity. Supplier and CloudNuro will not use Customer's name as a reference for marketing or promotional purposes.

EXHIBIT 3

Cook County IT Special Conditions (ITSCs)

Exhibit 3

Cook County Information Technology Special Conditions (ITSCs)

1. DEFINITIONS FOR special conditions

1.1. ***"Biometric Information"*** has the same meaning as "biometric information" defined in the Illinois Biometric Privacy Act, 740 ILCS 14/10.

1.2. "***Business Associate Agreement***" or "***BAA***" means an agreement that meets the requirements of 45 C.F.R. 164.504(e).

1.3. ***"Cardholder Data"*** means data that meets the definition of "Cardholder Data" in the most recent version of the Payment Card Industry's Data Security Standard.

1.4. ***"Contractor"*** has the same meaning as either "Contractor" and "Consultant" as such terms are defined, and may be interchangeably used in the County's Professional Services Agreement, or "Contractor" as defined in the County's Instruction to Bidders and General Conditions, if either such document forms the basis of this Agreement. "Contractor" includes any individuals that are employees, representatives, subcontractors or agents of Contractor.

1.5. "***Contractor Confidential Information***" means all non-public proprietary information of Contractor that is marked confidential, restricted, proprietary, or with a similar designation; provided that Contractor Confidential Information excludes County Data or information that may be subject to disclosure under Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or other law.

1.6. "***County***" has the same meaning as the term "County" in the Cook County Procurement Code, located at Chapter 34, Article IV in the Cook County Code of Ordinances as amended.

1.7. "***County Confidential Information***" means all non-public proprietary information of County, including Personally Identifiable Information and any information that is exempt from public disclosure under the Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances.

1.8. "***County Data***" means all data, including County Confidential Information, provided by the County to Contractor, or otherwise encountered by Contractor for purposes relating to this Agreement, including related metadata.

1.9. "***County Intellectual Property***" or ***"County IP"*** means all Intellectual Property owned or licensed by the County, including Developed IP.

1.10. "***Criminal Justice Information***" means data that meets the definition of "Criminal Justice Information" in the most recent version of FBI's CJIS Security Policy and also data that meets the definition of "Criminal History Record Information" at 28 C.F.R. 20.

1.11. "***Data Protection Laws***" means laws, regulations, industry self-regulatory standards, and codes of practice in connection with the processing of Personally Identifiable Information, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320(d) et seq.), the Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. § 17921 et seq.), FBI CJIS Security Policy, the Illinois Biometric Privacy Act, 740 ILCS 14/1, et seq., the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq., and the Payment Card Industry Data Security Standard..

1.12. ***"Data Breach"*** means (a) the loss or misuse (by any means) of any County Confidential Information; (b) the unauthorized or unlawful access, use, or disclosure of any County Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity or availability of any County Confidential Information.

1.13. ***"Deliverable"*** has the same meaning as "Deliverable" as defined in the County's Professional Services Agreement or as defined in the County's Instruction to Bidders and General Conditions, if either such document forms the basis of this Agreement.

1.14. "***Developed Intellectual Property***" or ***"Developed IP"*** means Intellectual Property conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services, including, but not limited to: (a) modifications to, or enhancements (derivative works) of, the County IP; (b) Developed Software; and (c) modifications to or enhancements (derivative works) of, Third Party Intellectual Property to the extent not owned by the licensor of the Third Party IP under the terms of the applicable license.

1.15. "***Intellectual Property***" or ***"IP"*** means any inventions, discoveries, designs, processes, software, documentation, reports, and works of authorship, drawings, specifications, formulae, databases, algorithms, models, methods, techniques, technical data, discoveries, know how, trade secrets, and other technical proprietary information and all patents, copyrights, mask works, trademarks, service marks, trade names, service names, industrial designs, brand names, brand marks, trade dress rights, Internet domain name registrations, Internet web sites and corporate names, and applications for the registration or recordation of any of the foregoing.

1.16. "***Malware***" means any hidden files, automatically replicating, transmitting or activating computer program, virus (or other harmful or malicious computer program) or any equipment-limiting, Software-limiting or Services-limiting function (including, but not limited to, any key, node lock, time-out or similar function), whether implemented by electronic or other means.

1.17. ***"Open Source Materials"*** means any Software that: (a) contains, or is derived in any manner (in whole or in part) from, any Software that is distributed as free Software, open source Software, shareware (e.g., Linux), or similar licensing or distribution models; and (b) is subject to any agreement with terms requiring that such Software be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributable. Open Source Materials includes without limitation "open source" code (as defined by the Open Source Initiative) and "free" code (as defined by the Free Software Foundation).

1.18. "***Personally Identifiable Information***" means personal data or information that relates to a specific, identifiable, individual person, including County personnel. For the avoidance of doubt, Personally Identifiable Information includes the following: (a) any government-issued identification numbers (e.g., Social Security, driver's license, passport); (b) any financial account information, including account numbers, credit card numbers, debit card numbers, and other Cardholder Data; (c) Criminal Justice Information; (d) Protected Health Information; (e) Biometric Information; (f) passwords or other access-related information associated with any user account; and (g) any other personal data defined as personally identifiable information under the breach notification laws of the fifty states.

1.19. "***Protected Health Information***" or "***PHI"*** has the same meaning as the term "Protected Health Information" in 45 C.F.R. 160.103.

1.20. "***Services***" has the same meaning as "Services" as defined in Article 3 of the County's Professional Services Agreement or "Deliverables" as defined in the County's Instruction to Bidders and

General Conditions, if either such document forms the basis of this Agreement.

1.21. "***Software***" means computer programs, whether in source code or object code form (including any and all software implementation of algorithms, models and methodologies), databases and compilations (including any and all data and collections of data), and all documentation (including user manuals and training materials) related to the foregoing.

2. SERVICES AND DELIVERABLES

2.1. Approved Facilities. Contractor will perform Services and host County Data only within the continental United States and only from locations owned, leased or otherwise used by Contractor and its Subcontractors.

2.2. Required Consents for Assets in Use and Third-Party Contracts as of the Effective Date**.** For this section, "Assets" mean equipment, Software, Intellectual Property and other assets used in providing the Services and "Required Consent" means the consent required to secure any rights of use of or access to any of County-provided or third-party Assets that are required by Contractor to perform the Services. Contractor is responsible for obtaining all Required Consents relating to this Agreement. The County will cooperate with Contractor and provide Contractor such assistance in this regard as the Contractor may reasonably request.

2.3. Resources Necessary for Services. Except as set forth in this Agreement, Contractor will provide and is financially responsible for all equipment, Software, and other resources needed to perform the Services in accordance with the Agreement.

3. LEGAL COMPLIANCE

3.1. Public Records Laws. Contractor will comply with all laws governing public records located at 50 ILCS 205/1 et seq. and at 44 Ill. Admin. Code 4500.10 et seq. Specifically, and without limitation, Contractor must: (a) store County Data in such a way that each record is individually accessible for the length of the County's scheduled retention; (b) retain a minimum of two total copies of all County Data according to industry best practices for geographic redundancy, such as NIST Special Publication 800-34 as revised; (c) store and access County Data in a manner allowing individual records to maintain their relationships with one another; (d) capture relevant structural, descriptive, and administrative metadata to County Data at the time a record is created or enters the control of Contractor.

3.2. Data Protection Laws. Contractor will comply with all applicable Data Protection Laws, including those that would be applicable to the Contractor if it, rather than the County, were the owner or data controller of any County Data in its possession or under its control in connection with the Services.

3.3. Export Laws. Contractor will comply with all laws governing the export of intellectual property, including, but not limited to the Export Administration Regulations, 15 CFR 730, et seq.

3.4. Protected Health Information. If Contractor will have access to Personal Health Information in connection with the performance of the Services, Contractor must enter a Business Associate Agreement in a form provided by the County. See Attachment X, Business Associate Agreement.

3.5. Criminal Justice Information. If Contractor will have access to Criminal Justice Information in connection with the performance of the Services, Contractor must execute an FBI CJIS Security Policy Addendum or any other required agreements in a form provided by the County. See Attachment X, CJIS Security Policy Addendum.

3.6. Biometric Information. If Contractor will have access to Biometric Information in connection with the performance of the Services, Contractor must properly secure such information in compliance with the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq., including maintaining a retention schedule and destruction guidelines.

3.7. Cardholder Data. If Contractor will have access to Cardholder Data in connection with the performance of the Services, no less than annually, Contractor must tender to County a current attestation of compliance signed by a Qualified Security Assessor certified by the Payment Card Industry.

4. WARRANTIES

4.1. Contractor Materials and Third Party IP. Contractor represents and warrants that it owns, or is authorized to use, all Contractor IP, and Contractor-provided third-party IP.

4.2. Developed Software. Contractor represents and warrants that all developed software will be free from material errors in operation and performance, will comply with the applicable documentation and specifications in all material respects, for twelve (12) months after the installation, testing and acceptance of such developed software by the County. Any repairs made to developed software pursuant to this Section will receive a new twelve (12) month warranty period in accordance with the terms of this Section.

4.3. Open Source Materials. Contractor represents and warrants that all open source materials (OSM) included in Deliverables or Software are obtained from a trusted distributor. Unless otherwise specified in this Agreement, Contractor must maintain OSM support, including required patching and security updates, which will be provided promptly after release. The Contractor must not use any materials that allow users to modify or incorporate open source code into larger programs on the condition that the software containing the source code is publicly distributed without restrictions, commonly known as "copyleft."

4.4. Access to County Data. Contractor represents and warrants that Contractor has not and will not prevent, or reasonably fail to allow, for any reason including without limitation late payment or otherwise, the County's access to and retrieval of County Data.

4.5. Malware. Contractor represents and warrants that it has not and will not introduce or cause to be introduced Malware in any County IT environment at any time. If Contractor discovers that Malware has been introduced into Software, Contractor must, at no additional charge, (a) immediately undertake to remove such Malware (b) notify the County in writing within one (1) business day, and (c) use reasonable efforts to correct and repair any damage to County Data or Software and otherwise assist the County in mitigating such damage and restoring any affected Service, Software or equipment.

4.6. Resale of Equipment and Software. If Contractor resells to the County any equipment or Software that Contractor purchased from a Third Party, Contractor, to the extent it is legally able to do so, must pass through any such third-party warranties to the County and reasonably cooperate in enforcing them. Such warranty pass-through will not relieve Contractor from its warranty obligations set forth in this Section.

4.7. Data Security. Contractor represents and warrants that (a) it will not permit any unauthorized access to or cause any loss or damage to County Data or County IP; (b) it will comply with all County security policies in place during the term of this Agreement, and (c) it will not use any system that is dependent on software or hardware that no longer have appropriate security updates available.

5. INTELLECTUAL PROPERTY

5.1. County Intellectual Property. The County retains all right, title and interest in and to all County IP. Contractor will not be permitted to use any of the County IP for the benefit of any entities other than the County. Upon expiration or termination of this Agreement, Contractor must cease all use of County IP and must return to the County all County IP.

5.2. Developed Intellectual Property. Contractor hereby irrevocably and unconditionally assigns, transfers and conveys to the County without further consideration all of its right, title and interest in such Developed IP, which assignment will be effective as of the creation of such works without need for any further documentation or action on the part of the Parties. Contractor agrees to perform any actions as may reasonably be necessary, or as the County may reasonably request, to perfect the County's ownership of any such Developed IP.

5.3. Residual Knowledge. Nothing contained in this Agreement will restrict either Party from the use of any ideas, concepts, know-how, or techniques relating to the Services which either Party, individually or jointly, develops or discloses under this Agreement, provided that in doing so (a) such information is solely retained in the unaided memory of the Parties employees performing or using such Services, (b) the Party does not breach its respective obligations under Section 6 relating to confidentiality and non-disclosure, and (c) does not infringe the Intellectual Property rights of the other or Third Parties who have licensed or provided materials to the other. Except for the license rights contained under Section 5, neither this Agreement nor any disclosure made hereunder grants any license to either Party under any Intellectual Property rights of the other.

5.4. Software Licenses. This Agreement contains all terms and conditions relating to all licenses in Contractor-Provided Software and Contractor IP. Except as explicitly set forth elsewhere in this Agreement, all licenses that Contractor grants in Contractor-Provided Software include: (a) the right of use by Third Party Contractors for the benefit of the County, (b) the right to make backup copies, and (c) the right to reasonably approve the procedures by which Contractor may audit the use of license entitlements.

6. COUNTY DATA AND CONFIDENTIALITY

6.1. Property of County. All County Data is the sole property of the County. Contractor must not use County Data for any purpose other than that of performing the Services under this Agreement. Without the County's express written consent, no County Data, or any part thereof, may be disclosed, sold, assigned, destroyed, altered, withheld, or otherwise restricted by Contractor or commercially exploited by or on behalf of Contractor.

6.2. Acknowledgment of Importance of County Data. Contractor acknowledges the importance of County Data and that the County may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement.

6.3. Data Recovery. Upon the County's request Contractor must promptly return all requested County Data to the County or its designee in such a format that the County may reasonably request. Contractor must provide County with adequate bandwidth and other resources to remove County Data from Contractor servers. Contractor must also provide sufficient information requested by the County about the format and structure of the County Data to enable such data to be used in substantially the manner used by Contractor. Also upon County's request, in lieu of return or in addition to return, Contractor must destroy County Data, sanitize any media upon which County Data resides in accordance to NIST Special Publication 800-88 as revised; and upon County request, Contractor must provide County with a certificate of destruction in compliance with NIST Special Publication 800-88.

6.4. Disclosure Required by Law, Regulation or Court Order. In the event that Contractor is required to disclose County Data in accordance with a requirement or request by operation of Law, regulation or court order, Contractor will, except to the extent prohibited by law: (a) advise the County thereof prior to disclosure; (b) take such steps to limit the extent of the disclosure to the extent lawful; (c) afford the County a reasonable opportunity to intervene in the proceedings; and (d) comply with the County's requests as to the manner and terms of any such disclosure.

6.5. Data Integrity and Loss of County Confidential Information. Data integrity requires that data are complete, consistent, and accurate. As appropriate Contractor must implement and maintain strong, industry standard measures, such as encryption, cryptographic key systems, digital signatures, and firewalls, to maintain accuracy of County Data. Without limiting any rights and responsibilities under Section 7 of these IT Special Conditions, in the event of any disclosure, inaccuracy, or loss of, or inability to account for, any County Confidential Information, Contractor must promptly, at its own expense: (a) notify the County in writing within one (1) business day; (b) take such actions as may be necessary or reasonably requested by the County to minimize the violation; and (c) cooperate in all reasonable respects with the County to minimize any damage resulting from the violation.

6.6. Contractor Confidential Information. County must use at least the same degree of care to prevent disclosing Contractor Confidential Information to Third Parties as County exercises to avoid unauthorized disclosure, publication or dissemination of its County Confidential Information of like character.

7. DATA SECURITY AND PRIVACY

7.1. General Requirement of Confidentiality and Security. Contractor is obligated to maintain the confidentiality and security of all County Confidential Information in connection with the performance of the Services. Without limiting Contractor's other obligations under this Agreement, Contractor must implement and/or use network management and maintenance applications and tools, appropriate fraud prevention and detection and encryption technologies to protect the aforementioned; provided that Contractor must, at a minimum, encrypt all Personally Identifiable Information in-transit and at-rest. Contractor must perform all Services using security technologies and techniques in accordance with industry-leading practices and the County's security policies, procedures and other requirements made available to Contractor in writing.

7.2. Security. Contractor must establish and maintain reasonable and sufficient physical, technical and procedural safeguards to preserve the security and confidentiality of County Confidential Information and to protect same against unauthorized or unlawful disclosure, access or processing, loss, destruction or damage. The safeguards must provide a level and scope of security that is not less than the level and scope required under (a) the County Policies as updated; (b) Federal Information Processing Standard 200; (c) then-current NIST 800-series standard and successors thereto; or (d) an equivalent, generally accepted, industry-standard security standards series.

7.3. Contractor Personnel. Contractor will oblige its personnel to comply with applicable Data Protection Laws and to undertake only to collect, process or use any County Data necessary to perform the Services and not to make the aforementioned available to any Third Parties except as specifically authorized hereunder. Contractor must ensure that, prior to performing any Services or accessing any County Data or other County Confidential Information, all Contractor personnel who may have access to the aforementioned must have executed agreements concerning access protection and data/software security consistent with this Agreement.

7.4. Information Access. Contractor may not attempt to or permit access to any County

Confidential Information by any unauthorized individual or entity. Contractor must provide its personnel only such access as is minimally necessary for such persons/entities to perform the tasks and functions for which they are responsible. Contractor will, upon request from the County, provide the County with an updated list of those personnel having access to County Data and the level of such access.

7.5. Encryption Requirement. Contractor must encrypt all County Confidential Information. Contractor must encrypt the aforementioned in motion, at rest and in use in a manner that, at a minimum, adheres to NIST SP 800-111, NIST SP 800-52, NIST SP 800-77 and NIST SP 800-113 encryption standards. Contractor must not deviate from this encryption requirement without the advance, written approval of the County's Information Security Office.

7.6. Updates. Contractor must provide to County, without charge, the timely application of any upgrades to software required for Services that are available to third parties. Software upgrades must include, but not be limited to, new version releases and operating system patching, as well as bug fixes.

7.7. Contractor as a Data Processor. Contractor understands and acknowledges that, to the extent that performance of its obligations hereunder involves or necessitates the processing of Personally Identifiable Information, it will act only on instructions and directions from the County.

7.8. Data Subject Right of Access and Rectification. If the County is required to provide or rectify information regarding an individual's Personally Identifiable Information, Contractor will reasonably cooperate with the County to the full extent necessary to comply with Data Protection Laws. If a request by a data subject is made directly to Contractor, Contractor will notify the County of such request as soon as reasonably practicable.

7.9. Data Minimization. Contractor must implement procedures to minimize the collection of Personally Identifiable Information.

8. DATA BREACH

8.1. Notice to County. Contractor must provide the County with written notice of any Data Breach promptly following, and no later than one (1) business day following, the discovery or suspicion of the occurrence of a Data Breach. Such notice must summarize in reasonable detail the nature of the County Data that may have been exposed, and, if applicable, any persons whose Personally Identifiable Information may have been affected or exposed by such Data Breach. Contractor must not make any public announcements relating to such Data Breach without the County's prior written approval.

8.2. Data Breach Responsibilities. Upon discovery of an actual or reasonably suspected loss, or unauthorized use, access, or disclosure, of County Data, Contractor must promptly provide details regarding the incident, its mitigation efforts, and its corrective action to prevent a future similar incident. Contractor must fully cooperate with County, and is solely responsible for: (a) investigating and resolving any data privacy or security issue; (b) providing County with a root cause analysis of the breach, (c) notifying any affected persons (solely at County's direction) and governmental regulators, as applicable; and (d) recovering affected data or information, to the extent possible, and (e) provide County with a corrective action plan acceptable to County.

8.3. Notice to Impacted Parties. County has the sole right to determine (a) whether notice of the Data Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in County's discretion; and (b) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

8.4. Costs. In the event of a Data Breach attributable to an act or omission of Contractor, as part of such remediation, Contractor must pay all cost and expense of County's compliance with any of County's notification obligations, as well as the cost of credit monitoring services for affected individuals.

9. AUDIT RIGHTS

9.1. Service Organization Control (SOC 2), Type II Audits. Contractor must, at least once annually and at its sole cost and expense provide to the County and its auditors a SOC 2, Type II report, or equivalent, for all locations at which the County Data is processed or stored. Contractor must promptly make available to the County the results of any reviews or audits conducted by Contractor (including internal and external auditors), including SOC-2 audits, relating to Contractor's and its Subcontractors' operating practices and procedures to the extent relevant to the Services or any of Contractor's obligations under the Agreement.

9.2. Subcontractor Agreements. Contractor must ensure that all agreements with its Subcontractors performing Services under this Agreement contain terms and conditions consistent with the County's audit rights.

10. EXIT ASSISTANCE

10.1. Removal of Contractor Materials. Contractor is responsible, at its own expense, for de-installation and removal from the County facilities any equipment owned or leased by Contractor, that is not being transferred to the County under the Agreement, subject to the County's reasonable procedures and in a manner that minimizes the adverse impact on the County.

11. MISCELLANEOUS

11.1. Survival. Sections 1 (Definitions for Special Conditions), 5 (Intellectual Property), 9 (Data Breach), and 10 (Audit Rights) will survive the expiration or termination of this Agreement for a period of five (5) years (and Sections 6 (County Data and Confidentiality) and 13 (Miscellaneous) will survive for a period of ten [10] years) from the later of (a) the expiration or termination of this Agreement (including any Exit Assistance Period), or (b) the return or destruction of County Confidential Information as required by this Agreement.

11.2. No Limitation. The rights and obligations set forth in these IT special conditions exhibit do not limit the rights and obligations set forth in any Articles of the Professional Services Agreement. For the avoidance of doubt, the use of County in the PSA or GC will expressly include County and vice versa.

11.3. No Click-Wrap or Incorporated Terms. The County is not bound by any content on the Contractor's website, in any click-wrap or other similar document.

12. EPIDEMIC DISRUPTION

12.1. **Epidemic Disruption.** County may suspend Services under any Statement of Work on 2 business days' written notice in case of Epidemic Disruption (as defined below). Each party's deadlines and obligations related to performance, receipt, or support of Services will then be delayed by a period equal to the duration of such suspension, provided suspension will not delay Customer's obligations to make payments already due pursuant to the terms of this Agreement. County may end such suspension at any time on 5 business days' notice, provided Contractor may by prompt written notice delay such Services' restart date by up to 2 weeks if earlier return of staff imposes unreasonable burdens on Contractor. If performance pursuant to a Statement of Work is suspended due to Epidemic Disruption for more than 40 business days out of any 90-day period, either party may terminate such Statement of Work for convenience on 10 days' prior written notice, provided that if Provider issues such termination notice and County ends the suspension before the notice period ends, the Statement of Work will not terminate. For the avoidance of doubt: (a) termination pursuant to the preceding sentence does not release Provider from its obligations pursuant to PSA Section __ (*Transition Assistance*); and (b) nothing in this PSA Section __ limits either party's rights set forth in PSA Section __ (*Force Majeure*), including without limitation either party's right to suspend Services as a result of epidemics. ("Epidemic Disruption" occurs when County reasonably concludes (i) that risks related to an epidemic make performance, receipt, or support of Services unreasonably dangerous for either party's employees or for third parties or (ii) that government shelter-in-place orders or other government measures addressing an epidemic make performance, receipt, or support of Services unduly expensive or otherwise impractical.)

EXHIBIT 4

System Requirements Matrix

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their solution to the requirements specified in this workbook. This template must be completed and submitted as an MS Excel file as part of the response to this RFP.

- Assign a number value to each row in all tabs.

- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.

- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.

- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.

- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the

- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned	2 Not delivered; Meet via 3rd Party	1 Custom Code Require	Vendor Comments [Indicate how this requirement is achieved using which specific County owned Software or Vendor suggested new software]
1.0	**Solution Platform**						
1.1	Solution platform shall have standards based interoperability between its various components such as but not limited to User credential store(s), Business process flow, Federation server, Policy design/enforcement, monitoring, Cisco ICE	5					Oracle Identity Governance(OIG) and Oracle Access Manager(OAM) have standards-based interoperability. **OAM:** It supports standard integration to onboard application based on SAML, OIDC, and HearderBased integration standards. OAM's orchestration helps design business process flow. **OIM:** It supports direct integration with target applications (List of connectors: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/) , the connector also supports standard integrations like Generic SCIM, FlatrFile, Database, REST, etc.
1.2	Solution platform shall have business process flows for user and application on-boarding and off-boarding functions		4				**User and application Onboarding:** There are multiple ways users can be onboarded using OIM12c. 1. Using trusted reconciliation 2 Starting from OIM web console 3 OIM provided REST API's. OIM 12c providers connectors for integration with different type of target systems. With 12c OIM application on-boarding has been simplified for Admins and it allows cloning as well as developing templates for onboarding similar type of applications. Application onboarding can be used to create templates for connected as well as disconnected applications. 12c OIM provides configuration options to add approver details as well as risk classifications for Applications as well as Entitlements. 12c OIM has different roles for different functionalities, application admin role can be leveraged to allow application owners to create applications with required mappings. **User and Application offboarding/Retirement:** Users can be offboarded in multiple ways and the following is a common example.1.Based on termination status coming from Trusted source (typically a HRMS application)2.Admin/Manager terminating user from OIM web console. . With respect to application offboarding There are more ways in Based on business needs custom process can be defined to offboard an application to ensure that it is not available for requesting, provisioning, reconciliation or review certification check. This application is not completed removed from OIM environment; it will be available only to OIM Admins for Audit purposes after it has been retired.
1.3	Soltuion platform implementation shall support best practices for change management procedures		4				Both OAM and OIM can be configured to seamlessly propagate changes/changes across multiple platforms. OIM provides import and export utility where as OAM provides T2P (Test to production) utility. Extensive REST API's provided by OAM and OIM can be leveraged in DevOps for easy configuration migration.
1.4	Solution platform shall support for user data stores at a minimum but not limited to Microsoft AD, Application Databases, Oracle Unified Directory	5					OIM could use its connector framework to provision the user data to systems like Microsoft AD, Application Databases, Oracle Unified Directory and other applications.
1.5	Solution platform shall have a master user data store with replication between its participating agency user data stores		4				OIM will be the master user repository which will take data from all trusted sources and will push all new user and data updates to all target systems
1.6	Solution platform shall have master federation server trust working with optional agency owned federation server(s)					1	The Oracle access manager will be the master federation server which will act as IDP and SP based on the application integration. OAM and agency owned federation server(s) with work together to provide a seamless SSO experience.
1.7	Solution shall have central policy definition tool set	5					Oracle Access Manager (OAM) provides a central policy definition for authentication and authorization services.
1.8	Solution platform shall have data enryptions at rest and in-transit	5					All in-transit communication will be over SSL where as all the sensitive information that is stored in the LDAP and database will be encrypted.
1.9	Solution platform implementation shall support agency on-boarding activities such as but not limited to integraing user data stores, data sync, application on-boarding, approval framework for agency users.	5					OIM supports direct integration with target applications (List of connectors: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/) , the connectors framework also supports standard integrations like Generic SCIM, FlatFile, Database, REST, etc. OIM's reconciliation engine handles user and entitlement data synchronization. Using SOA it is very easy to create new approval workflows and attach them to the application, role, entitlement, etc.
1.10	Solution platform implementation shall support agency off-boarding activities such as but not limited to disconnecting user data stores, disable data sync, application off-boarding, disable approval framework for agency users.	5					In OIM, admins can disable provisioning, disable data sync (by disabling schedule tasks), removing approvals by modifying approval policies.
1.11	Solution platform shall have isolated administration access to support agency assets and central platform	5					Delegating administration allows a high-level administrator to grant responsibilities to other, more local administrators. When you delegate administration, you determine what rights you want to grant to another user. A Super/System Administrator can grant the rights to administer an Application Domain to an Application Domain Adminstrator. An Application Domain Adminstrator can further delegate the rights to administer one or more of their Application Domains to other Application Domain Administrators. An Application Domain Administrator can create and edit Resources, Authentication Policies and Authorization Policies. These rights are scoped to one or more Application Domains.

1.12	Solution platform shall log all central administration tasks including but not limited to all CRUD functions	4	Oracle Identity Manager provides a powerful audit engine to collect extensive data for audit and compliance purposes. You can use the audit functionality together to capture, archive, and view entity and transactional data for compliance monitoring and IT-centric processes and forensic auditing.

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
2.0	**Policy Management & Governance**						
2.1	Vendor to review the County software list for Policy life cycle management. Provide the gap software list.						Privilege Account Management solution options would be discussed with CCG stakeholders and finalize the product / solution. For MFA using SMS, SMS provider options will be discussed and finalized duting design phase.
2.2	System shall have development tools for Policy Life Cycle management which includes Policy Creation, Policy Change Management, Policy Implementation, Policy Compliance and Audit.	5					Oracle Access Manager is a centralized policy manager where admins can create and update policies. These policies are enforced by webgate and OAM whenever application is accessed. Any changes to these policies are maintained in the audit
2.3	Policies shall be referenced by other policies and follow top down approach with County policies being more generic and agency specific polices be focused.		4				In Oracle access manager the policies in the application domain can be put in the order where these policies would be executed from top to bottom in the sequence. In addition Authentication levels, Adaptive authentication policies, and Authentication orchestration can be leveraged to enforce agency- policies.
2.4	Policy development shall make use of checklist-based requirements and implement reusable policy frameworks		4				Kapstone will leverage it's policy framework toolkit and present checklist options for Application integration, MFA, workflow, SoD, RBAC and others
2.5	System shall implement Password management policies	5					Both OIM and OAM has password policies
2.6	System shall implement Device usage policy – Location, Ownership, Network (public/private/county delegated/county owned)	5					OARM Policy will be configured to orchastrate access based on the device fingerprinting. Oracle Adaptive Access Manager contains proprietary clientless technologies for fingerprinting and interrogating devices used during access requests and transactions. Device fingerprinting is a mechanism to recognize the devices a customer uses whether it is a desktop computer, laptop computer or other web-enabled device. This appendix contains details about device fingerprinting.
2.7	System shall implement Allowed Devices policy	5					OARM policy can be defined based on the device categories.
2.8	System shall implement Applications access policy	5					OAM is the centralized authentication and authorization policy manager in which application access policy would be configured.
2.9	System shall implement User authentication Policy (User credentials, user to device relationship, multi-factor, user type – employee/contractor/citizen/vendor)		4				Oracle access manager will validate user credentials based on user type also OIM would use OAA (Oracle Advanced Authentication) for user to device relationship and multi-factor Oracle Advanced Authentication (OAA) is a standalone micro-service that supports establishing and asserting the identity of users. OAA provides strong authentication using Multiple Authentication Factors (MFA). A wide range of authentication (challenge) factors are available out-of-the-box for establishing the identity of users.
2.10	System shall be compliance to Federal, State and Local laws, including FERPA, GLBA and ADA Section 508.		4				Kapstone will configure solution adhering to compliance requirements wherever possible.
2.11	System shall have Policy attributes to define complexity, priority, importance. Applicable policy can be selected from the policy hierarchy. (For example, Password change policy could be defined at county level, at agency level or at department level. These attributes would define the system rules to select the policy by default and allows overrides if any)	5					Oracle access manager has policy orchestration in which admin can define what need's to happen during authentication flow. Ex: If the user is Employee then authenticate against AD and if the contractor then authenticates against OUD after this validate agency level and department. This can be achieved in orchestration.

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments [Indicate how this requirement is achieved using which specific County owned Software or Vendor suggested new software]
3.0	**Integrations & Connectors**						
3.1	System shall have support for providing and consuming REST services	5					Both OIM and OAM provides REST services to support different operations like REST API's for user CRUD operation, application onboarding, policy management, etc. Most PAM vendors provide REST APIs. Kapstone will make sure to evaluate PAM solution that meets CCG requirements
3.2	System shall have support for providing and consuming Web services.	5					Both OIM and OAM provides REST services to support different operations like REST API's for user CRUD operation, application onboarding, policy management, etc.
3.3	Vendor shall identify all connectors/adapters for interfaces, provide the list by source/target application		4				This can be identified during requirement gathering.
3.4	System shall have development tools to connect to listed applications.		4				Oracle and PAM vendors supports multiple interfaces to connect e.g. JDBC, REST, Web UI, SSH, SFTP. Kapstone will work with CCG architecture team to finalize the client tool list. OIM had many direct connector(List of connectors: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/), these direct connector and generic connector framework can be used to provision users to their attributes to the County/Agency assigned applications.
3.5	Vendor shall identify specific integration tool from the county software list to be used with Identity and Access management solution. Provide the merits for the same.		4				Kapstone will work with CCG team to prepare inventory of integration tools used in CCG environment. Kapstone would provide recomendations for the each interface. e.g. Oracle IAM solutions can be managed using WEB UI, REST APIs (leverage postman or CURL), Oracle Database (can be accessed using Oracle SQL Developer, Toad), Ant script for offline or command line admin activities, Jenkins or Councourse can be used for CICD, Container engineer can be managed usign OKE, Open Shift, Tanzu.
3.6	Vendor shall provide any gap software for developing the needed interfaces with County applications list.	5					Kapstone will provide the list of software once detailed requirement gathering anf high level solution is finalized
3.7	Vendor solution shall implement below system interfaces						
3.7.1	a) MS MIM		4				MIM will be configured with OIG as trusted or can be used as target system. Co-existance between OIG and MIM will be configured
3.7.2	b) Cisco ISE		4				EIAM solution will be configured to work with CISCO ISE for SSO integrations or Identity Sync.
3.7.3	c) Oracle HCM		4				OIG will be configured as trusted and target system
3.7.4	d) MS O365		4				EIAM solution will be integrated with Office 365 (OIG for Provisioning, OAM for Federation, PAM for managing system accounts)
3.7.5	e) Oracle OAG/OIF		4				Oracle API gateway can be integrated using OAM and OUD. OIF can be integrated with OAM 12. OIF fucntionality is convered into OAM 12c except ws-fed, based on the requiremetn gathering OIF fucntions can be migreated to OAM.
3.7.6	f) DBs – Oracle and SQL Server		4				IGA , PAM can be configured for DB Account & Entitlement managements. OUD adapters can be configured for delegated password validation.
3.7.7	g) SIEM		4				EIAM will be configured to integrate with SIEM tool for centralized log management and optionally for consolidated auditing.

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party	1 Custom Code Required	Vendor Comments
4.0	**User On/Off-Boarding**						
4.1	Vendor shall review the County application software list for implementing a workflow included business processes for County and its agencies. Provide the gap software list.		4				It will be provided during first couple of months of project
4.2	System shall support users of types including but not limited to, county employees, county contractors, (Citizens), vendor users doing business with county.		4				OIM support not only creation of custom user types but it also supports creating business process per user type
4.3	System shall have user on-boarding policies defined by business function such as agency, department, others.		4				In OIM we can define user onboadring process per user type. For ex. user email would be based on user type also they may have access to different application
4.4	System shall define basic user profile with all attributes common to as county employee, add agency specific attributes to the user profile		4				We can defind user defind field in the user profile these field can be used to store agency specific attributes.
4.5	System shall define the On-Boarding process by user type		4				In OIM we can define user onboadring process per user type. For ex. user email would be based on user type also they may have access to different application
4.6	System shall identify the user attributes by user type		4				OIM can auto populate user attributes bases on user type and/or other attributes
4.7	System shall interface with County/Agency assigned applications for User attribute provisioning		4				OIM had many direct connector(List of connectors: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/), these direct connector and generic connector framework can be used to provision users to their attributes to the County/Agency assigned applications.
4.8	System shall have common reusable API to sync user attributes with all interfaced applications.		4				OIM connector can be configured to use reusable API to sync user attributes
4.9	System shall have user provisioning by role-based approval process defined at County, agency and Department level		4				OIM can use multiple attributes (County, agency, Department level, etc.) to assign a user to a role and provision a user to the application.
4.10	System shall initiate tasks for manual steps and manual reviews, track the outcomes and generate user provisioning report from end to end.		4				OIM does create the task for manual fulfillment some task needs to be completed manually moreover if provisioning tasks fail it can assign a task to the admin
4.11	System shall escalate the user provisioning timed tasks defined by the policy		4				Admin can easily configure the escalation process in the approval workflow and the certification. One of the common configurations that companies would use is that if the manager is not able to take a action on the request within a predefined timeline then automatically escalate the request and assign it to the manager's manager.
4.12	System shall have defined change management process for Central business process workflow with all agencies as approval stake holders		4				Kapstone will work with CCG team to define Change management process. EIAM solution out of the box provide Role and access policy governance process. In addition, impact analysis options of EIAM solutioon can be leveraged to setup stakeholder approvals. Object definition access reviews can be leverahged to periodically review and approve policy definitions.
4.13	System shall provide User Profile query API	5					There are multiple ways to check user profile. 1. OIM Admin console (Preffered) 2. Using REST API's 3. Using SDK 4. Database query
4.14	System shall provide access to profile query API by defined policies.	5					OIM Provides the REST API's and SDK's to get details of user, role, catalog, policy, etc.
4.15	System shall send notifications to User profile changes such as automated system mass updates,		4				OIM system can send notifications whenever a user is created or updated in OIM.
4.16	System shall define and implement password change policies		4				Admins can define password policy in OIM. This will be used by OIM to generate random passwords for a new user, also the same password policy will be used when the user is trying to change their password .

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their solution to the requirements specified in this workbook. This template must be completed and submitted as an MS Excel file as part of the response to this RFP.

- Assign a number value to each row in all tabs.

- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.

- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.

- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.

- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the

- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date.	Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments [Indicate how this requirement is achieved using which specific County owned Software or Vendor suggested new software]
5.0	**Authentication & Authorization**						
5.1	System shall authenticate users with at least two factors using combination of knowledge factors, possession factors and or inference factors. Vendor response to include any third party authentication methods.	5					OAM will be integrated with Oracle Advanced Authentication (OAA). OAA provides strong authentication using Multiple Authentication Factors (MFA). A wide range of authentication (challenge) factors are available out-of-the-box for establishing the identity of users.
5.2	System shall have features to support multiple authentication options including but limited to - County provided credentials, Social logins with Facebook, google, Microsoft and other trusted identity providers.		4				OAM ships an out-of the box OIDC Client Authentication Plugin, OpenIDConnectPlugin that enables integration with Social Identity providers such as IDCS, Google and Facebook. Apart from being an OAuth/OpenIDConnect2.0 Server, Oracle Access Manager (OAM) can also delegate authentication to OpenIDConnect-Social Identity Providers such as IDCS, Google, Facebook or even OAM itself, thus behaving like a relying party (service provider). After authenticating the user, the IDP redirects back to OAM where the user is asserted by OAM and an OAM Session is created.
5.3	System shall do Identity mapping of user attributes to identify the unique user. Identity attributes including but not limited to County issued Employee Number, Email Address, System Generated Unique ID.		4				OAM can use different authentication schemes to authenticate users, one authentication schem can use user-login and the other can use an email address as user idenfier
5.4	System shall create and manage Security Assertion Markup Language tokens (SAML)	5					OAM supports SAML protocol.
5.5	System shall have options to determine the Identity provider. Option include but not limited to, other federation server sources, a web page to select from, a trusted application.	5					Admin can create an authentication policy based on the application. For Example: If a user is trying to access the HR portal then allow them to login from Azure, if the user trying to access the contractor portal then give them a form login, etc.
5.6	System shall support user Internet Explorer, Firefox, Chrome and Safari browsers	5					Oracle IAM solution supports Internet Explorer, Firefox, Chrome and Safari browsers
5.7	System shall support user device OS including Windows, iOS, Android and Linux.	5					Oracle IAM web interfaces supports Windows, iOS, Android and Linux OS. Oracle Mobile authenticator supports Windows, Android and IOS devices.
5.8	System shall support Protocols and standards including but not limited to SAML, OAuth, OpenID Connect, Kerberos, SCIM, LDAP, REST, HTTP Post and Web Services.	5					Our solution supports SAML, OAuth, OpenID Connect, Kerberos, SCIM, LDAP, REST, HTTP Post and Web Services.
5.9	System shall support the creating and enforcing password management policies.	5					Admins can define password policy in OIM. This will be used by OIM to generate random passwords for a new user, also the same password policy will be used when the user is trying to change their password .
5.10	System shall provide auditing and logging from end to end including but not limited to activities such as navigating across applications, successful and failed log in attempts, session log off.		4				Oracle Access Manager uses the Oracle Fusion Middleware Common Audit Framework to support auditing for a large number of user authentication and authorization run-time events, and administrative events (changes to the system). The Oracle Fusion Middleware Common Audit Framework provides uniform logging and exception handling and diagnostics for all audit events.
5.11	System shall provide alerts and notifications for system configuration threshold monitoring.		4				Oracle IAM solution alerts and notifications will eb defined leveraging management pack. In addition, container engine (e.g. OKE or Azure K8s) can be leveraged to monitor infrastructure. Cloud native monitoring solutions like cloud guard and grafana canbe configured to monitor system health.
5.12	System shall support the Employees ~ 22000, Citizen users ~ 250 K, average number of logins in a day ~ 800, Number of applications – 15.		4				Our solution will be configured to support the Employees ~ 22000, Citizen users ~ 250 K, average number of logins in a day ~ 800, Number of applications – 15.
5.13	System shall allow protocol bridging, including but not limited to options such as SAML to OAuth to SAML	5					Our solution supports SAML, Oauth, OIDC, and Header based integration
5.14	System shall identify the user type such as privileged user, external user, internal county user		4				OAM authentication plug-in can be configured to call LDAP or database to find out if the user is a privileged user, external user, or internal county user.
5.15	System shall identify the authentication policies based on at a minimum user type and application type		4				OAM authentication orchestration process can be configured to take decisions bases on user type, application type, and other user attributes

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party solution
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
6.0	**Application On/Off-Boarding**						
6.1	Vendor shall review the County application software list for implementing a workflow included business processes for County and its agencies. Provide the gap software list.		4				OIG provide enterprise grade SOA for workflow management and it should be able to address CCG requirements. Kapostone will review CCG workflow requirements in detail during discovery phase and perform gap analysis to provide the list of software needed.
6.2	System shall provide a central business process with workflow tasks for application on-boarding and off-boarding.		4				Application on-boarding can be integrated based on the integratino patterns.
6.2.1	a) System shall include policies		4				Oracle IAM solution provide the polict orchastrations.
6.2.2	b) System shall include check lists		4				Oracle IAM provide the options to integrate applications for authentication and authroizations requirements. In addition, Kapstone developed application on-baording framework for application owner self-service.
6.2.3	c) System shall define access management roles for application management		4				Yes, Kapstone will provide best practices and standards to define role for authorizations including access approval policy.
6.2.4	d) System shall define privileged users for an application		4				Application Admin can be created which will have access to respective application.
6.3	System shall have query API for applications, access given based on defined policy for application attributes, user profile common attributes		4				Oracle provide JAVA SDK, DB interface, LDAP interface, SCIM Interface, and REST API to query required information. In addition, authorization can be applied for application specific access controls.
6.4	User authentication Policy vs Application authentication policy		4				Global user authentication policy can be confgiured based on the authewntication mechanism.User Authentication policy canbe configured based on user is authenticated using social login, Idp like Azure AD, native authentications. Additional step-up or Application authentication policy can be defined based on the authentication requirements (e.g. additional factor or only allowed second factor ...)
6.5	Application specific user attributes definition and management		4				OIG and OUD can be confgured for Application attribute on-boarding framework.
6.6	Authentication token provision and validation		4				OAM will configured to meet this requirement
6.7	Application authorizations management e.g. Oracle EBS		4				OIM and OAM will be configured to meet this requirement.
6.8	One ID access for County Web Applications		4				Kapstone will prepare inventory of applications and authentication mechanisms. Kapstone will develop registration and user on-boarding process including Oracle HCM or identity proofing integrations. Multiple options can be provided to link exisitng accounts using common attributes or providing merge account features or using link account options.
6.9	One-to-One mapping of a user identity between two servers so that the proper authorization decisions are made by downstream servers		4				It's out of the box IAM feature. In addition. coarsed grain can be confured in EIAM solution and delegated fine grained authorizations to target application.
6.10	Inbound Identity Mapping: Application specific, agency specific policies		4				Application on-boarding template will be provided to define attribute mapping and CICD & DevOps process will automate the configurations tasks
6.11	Outbound Identity Mapping: Application specific, agency specific policies		4				Application on-boarding template will be provided to define attribute mapping and CICD & DevOps process will automate the configurations tasks
6.12	Estimate should be based on Up to 5 applications integrated into IAM. Please also specify estimates for any additional application if identified later		4				For SSO application on-boarding, integration pattern will be defined. Kapston's factory model will on-board 5 applications andn based on the learning of first pilot application on-boarding, process be documented and automated. Application on-boarding time will vary based on the category of integration and application attribute mapping requirements. Kapstone should be able to on-board first 5 applications in 12 weeks once environment build is completed. Subsequence application on-boarding should be significantly faster leveraging DevOps process. For IGA application on-boarding, generally 4 weeks would be enough time for custom connector development provided we have apropriate application API and other required access.

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party solution can
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
7.0	**Privileged Access Management**						
7.1	Shall natively integrate and interoperate with all Microsoft products and technologies including Active Directory, ADFS. Azure. SQL Server. SharePoint. Dynamic CRM. SCCM. etc.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.2	Shall support all Microsoft and other enterprise authentication technologies and standards (i.e. Windows authentication, Kerberos, NTLM, SAML, TLS/SSL, DTLS, smart card, virtual smart card, biometrics and credentials).		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.3	Shall implement granular privileged access policies and enforce these policies on all County systems from a single management platform independent of Microsoft Active Directory, local Linux security sub systems and other local authentication and authorization systems.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.4	PAM solution shall maintain at least "99.99%" availability.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.5	An Active/Active (desired) or Active/Standby solution is mandatory for high availability.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.6	The procured/implemented system is expected to be rolled out in successive phases. The integration and cut overs to the new solution will be phased in to minimally impact the specific agency operations.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.7	Vendor must provide a three-year road map for any new gap software being suggested for the overall solution to meeting the functionality.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.8	Vendors must provide hardware and software maintenance for each of the proposed solutions that needs to cover support for 24x7x4 (4 hours response time), 24x7xNBD (next business day), and 8x5xNBD (8 hours a day, 5 day service with next business day for replacement parts)		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.9	Provide secure administrative host (i.e. jump server) capability to provide single point of access to the County assets without being a single point of failure for this critical County functionality.		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement
7.10	Ability to perform sequential screen capture and full video recording		4				Ksptone wiil work with CCG architect team to finalize the PAM vendor based on CCG's requirement

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their solution to the

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party solution can meet the
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
8.0	**Cisco Identity Services Engine**						Kapstone and it's partner have reviewed the requirements and will meet all requirements. Resumes and brief overview of capabilties are provided in the RFP repsonse.
8.1	Professional services are required for detailed documentation, installation/deployment, configuration and testing for Cisco Identity Services Engine for Cook County wired and wireless access networks. The documentation should have as-built and as-installed (not generic) details of the solution deployed at Cook County.		4				
8.1.1	a) The solution consists of multiple ISE servers with dedicated personas.		4				
8.1.2	b) Deploy the latest stable version of Cisco ISE		4				
8.1.3	c) The guest wireless design solution is based on a foreign/guest anchor controller.		4				
8.1.4	d) Customization of ISE based guest portals		4				
8.1.5	e) Design and document a wireless BYOD solution based on Cisco ISE		4				
8.1.6	f) Integration of Cisco ISE with Cisco Prime Infrastructure 3.x		4				
8.1.7	g) Ensure that the network is stable after the deployment and provide post deployment support which includes		4				
8.1.8	h) Provide a customized training for day to day operational support. This training should be focused for Service Desk/Help Desk resources providing level 1 support to end users.		4				
8.1.9	i) End Points connecting to ISE – Laptops; Desktops; Network Printers; Network Cameras; Mobile Devices; Tablets; Handheld Devices; Network appliances like VPN gateway		4				
8.2	The Vendor must have proven experience of at least two Cisco ISE solution deployments with a minimum of 1000 endpoints within the last 3 years. Please provide two examples of engagements of similar scope and size that your organization has completed.	5					
8.3	The Vendor should have at least two resources in its resource pool with relevant certifications and proven experience of Cisco ISE deployments. Resources with CCIE certification will be given preference. The resource should have proven experience of designing and architecting complex networking solutions with proven experience of writing detailed HLD and LLD documents.	5					
8.4	The certified technical resource (with proven ISE deployment experience) working on this project is expected to work onsite (Cook County Chicago) for the duration of the project. Cook County will provide all relevant facilities for the resource (work area, laptops etc.)	5					

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of their

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments [Indicate how this requirement is achieved using which specific County owned Software or Vendor suggested new software]
9.0	**Reports**						
9.1	System shall produce scheduled reports, for category areas such as Functional, Operational and Security related.		4				All reports will be available in the BI Publisher where reports can be exported in Microsoft Excel and Adobe PDF.
9.2	System shall have ability to export reports into Microsoft Excel, Adobe PDF.	5					Admin can schedule the reports and send the reports in email in BI Publisher
9.3	System shall provide opt in for automated scheduled reports, send reports as email attachments		4				BI Publisher has more than 30 out of the box reports moreover admin can create custom
9.4	System shall generate data for and create a report to provide User activity traceability to identify the user actions/tasks including read access of the resources.		4				Oracle Access Management auditing provide access history of each web applications. PAM solution would provide access history for each PAM integrated applications including session recvording. Kapstone would work CCG architecture team to configure dataabse access auditing and LDAP access auditing. Kapstone would provide and siscuss the performance impact and resource requirement for each access auditing configurations and finalize the access auditing granularity for each environment as well for each componenet.
9.5	System shall generate data for and create User profile reports include at a minimum but not limited to Types and Number of accounts by the user, Applications accessed, devices used, locations and usage		4				kapstone will develop the required reports using EIAM solution
9.6	System shall generate data for and create Accounts reports – type of account (Citizen, employee, Service, etc.), ownership, counts		4				BI Publisher can generate the reports that can show all the accounts based on user and user type.
9.7	System shall have development tools to create and manage reports		4				BI plusher is the application where admin would create, manage, and schedule reports.
9.8	System shall have access management controls for reports. Reports are accessible to defined roles.						Admin can create a custom report and they can give access to a specific report to a defined role
9.9	In addition to the built-in and out of the box reports, County shall seek the vendor up to 25 custom reports.		4				It will be accomplished during the project execution
9.10	Platform set up shall include DB/Data warehouse to retain all available platform audit, application, OS logs and device activity from Cisco ISE.		4				CISCO ISE provide comprehesive data retention policy. In addition, ISE provide hardening and best practice to manage log levels, encryptions.

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to indicate the fit of

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or development.
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If the 3rd party
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments [Indicate how this requirement is achieved using which specific County owned Software or Vendor suggested new software]
10.0	**Identity Analytics [Very high important Capability]**	5					
10.1	Vendor shall review the county available software list for creating identity analytics solution, provide the list of gap software to meet the county requirements.	5					Oracle's Identity Role Intelligence microservice meet the role mining, role governance, role management, entitlement analysis requirements.
10.2	Advanced analytics: Risk scoring, Computation and analysis; Identity correlation and profiling; Behavioral and data analysis; Continuous monitoring and alerting; Data presentation and visualization; Analytic data such as rogue or outlier access identification, peer group analysis, risk scoring, orphaned and dormant account identification, and usage patterns provides context to help managers make faster, more-informed access review decisions.		4				Kapstone's rogue account management (high level overview is provided in RFP repsonse) toolkit will provide the required functions. Kapstone has developed this utility based on our multple state and local IAM deployments. Kapstone service & rogue account management utility provide various identity co-relations rules, workflow to assign rogue accounts to default owner, self-service to reassign rogue accounts, process to contineously discover new rogue accounts and check for ownership in external systems.
10.3	Auditing, Tracking, Tracing:		4				kapstone's Service & rogue account management toolkit will meet the requirements
10.3.1	a) Tracking user activity: Tracking user navigations across applications		4				This can be achieved with the help of SIEM tool.OAM can be configured for web application usage tracking or activity tracing.
10.3.2	b) Failed log-in attempts: Logging system events like failed attempts etc.	5					
10.3.3	c) Threshold failed attempt notifications: Alert the administration team on the failed attempt with details - user being tried, device, location - IP, etc.		4				Access management alerting can be configured in management pack. This can also be achieved with the help of SIEM tool.
10.3.4	d) SLA & Response time: Meeting the response times in rendering SSO session activities. Ability to set threshold limits and alert notifications		4				Access management alerting can be configured in management pack. This can also be achieved with the help of SIEM tool.
10.3.5	e) SIEM integration: Integrate to McAfee Enterprise Security Manager		4				SIEM tool will be integrated to collect EIAM solution logs and audit data.
10.4	Usage anomaly Identification Reports		4				OIRI would provide outliers access report. Access management patttern can be reported using SIEM tool.
10.5	Predictive Analytics		4				OIRI and OARM providfe predictive analytics capabilties for identity analytics and access management.
10.6	Alerts for shared resource usage patterns – Devices shared by multiple users; Users sharing new devices; User credentials shared on multiple devices					1	Custom reports will configured to meer this requirement based on the audit and logs.

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to
- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement. If
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuratio n	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
11.0	**Maintenance – Operations & Support**						
11.1	Configure reports and analytics to assist in operations support and proactive/preventive monitoring and to determine the solution critical path components of such activities as listed below:	5					Kapstone will configure Identity management pack to monitor the Oracle IAM solution. Kapstone will also setup granular performance monitoring measures to anticipate potential performance issues for Oralce IAM platform. Kapstone will work with CCG team to identify CCG's platform preference like application monitoring tools, DB monitoring tools, cloud infrastructure monitoing tool and configure thresholds, response time deviation etc.
11.1.1	a) Root Cause Analysis; Developing custom tools/scripts where applicable.	5					Kapstone will use the operations toolkit(e.g. SQL query's, logs, audit data, Standalone progam) to find our the root cause of the issue.
11.1.2	b) Ticket resolution.	5					Kapstone team will work on any issues that are in scope
11.1.3	c) Platform maintenance and upgrades, timely applying critical security, application, DB and OS patches	5					Kapstone team will make sure that EIAM, CISCO ISE, PAM tools are timely patched . Fot the DB and OS patches we will work with CCG's respective team.
11.1.4	d) Systems availability monitoring		4				Kapstone will implement management pack and native monitoring tools that will monitor application also cloud monitoring tool can be used to monitor containers. Kapstone will work with CCG team to identify enterprise tools to define application monitoring, cloud infrastructure monitoring.
11.1.5	e) System access breach notifications					1	Kapstone will work with CCG team and vendor to identify events and define communication strategies. This cwould involve co-ordination among multiple teams and configurations of tools like SIEM tool, vedor provided updates, enterprise tools like threat detections, UEBA and etc.
11.1.6	f) Alerts and Escalations		0			1	Kapstone will work with CCG team and vendor to identify events and define communication strategies. This cwould involve co-ordination among multiple teams and configurations of tools like SIEM tool, vedor provided updates, enterprise tools like threat detections, UEBA and etc.
11.1.7	g) Stake holder communications		4				Kapstone project management methodogy will provide comprehensive communication strategy and plan.
11.1.8	h) Issue resolution include RCA and pattern identification.					1	Kapstone project management methodogy will provide comprehensive communication strategy and plan.
11.1.9	i) DR cycles		4				Kapstone will configure DR environemnt. kapstone will work with CCG team to finalize DR setup and testing strategies.
11.1.10	j) User activity alerts, where user performs activities occasionally or ad hoc basis					1	Kapstone will configure EIAM, CISCO ISE and PAM tool provided capabilties to identify anamolies. In addition. Kapstone will work with CCG team and vendor to identify events and define communication strategies. This cwould involve co-ordination among multiple teams and configurations of tools like SIEM tool, vedor provided updates, enterprise tools like threat detections, UEBA and etc.
11.1.11	k) Alerts for large query executions; Large import or export of files, data etc.					1	Kapstone will configure EIAM, CISCO ISE and PAM tool provided capabilties to identify anamolies. In addition. Kapstone will work with CCG team and vendor to identify events and define communication strategies. This cwould involve co-ordination among multiple teams and configurations of tools like SIEM tool, vedor provided updates, enterprise tools like threat detections, UEBA and etc.
11.1.12	l) Alerts for high volume (by transaction count or transaction volume) activity by single user or single device or single location.					1	Kapstone will configure EIAM, CISCO ISE and PAM tool provided capabilties to identify and report high volume transactions. In addition. Kapstone will work with CCG team and vendor to identify events and define communication strategies. This cwould involve co-ordination among multiple teams and configurations of tools like SIEM tool, vedor provided updates, enterprise tools like threat detections, UEBA and etc.
11.2	Regression test suite shall be created for automatic validation of the platform integrity and when new changes are deployed into production.					1	Kapstone will work CCG's standard regression testing tool. Some of the activities like ADF UI activities would require support for test suite administrator

RFP No. 2112-18598 - Enterprise Identity and Access Management (IAM) Implementation

Instructions

This workbook contains Functional, Proposal, and Technological Requirements for the system desired by Cook County. The response codes below should be used by responders to

- Assign a number value to each row in all tabs.
- A value of 5 states that the proposed solution can meet the functionality specified under Column B, right out of the box and will be available as soon as the software is installed.
- A value of 4 states that the proposed solution can meet the functionality specified under Column B, with some configuration work, but does not require custom code or
- A value of 3 states that the proposed solution will meet the functionality specified under Column B, with an expected new release of out of the box functionality.
- A value of 2 states that the proposed solution can not meet the functionality specified under Column B, but an existing 3rd party, compatible, solution can meet the requirement.
- A value of 1 states that the proposed solution can meet the functionality specified under Column B, with custom code or development.

Company Name	Kapstone, LLC

ID #	Requirements	5 Meets "Out of the Box"	4 Needs Configuration	3 Future Release Planned <Date, Version>	2 Not delivered; Meet via 3rd Party <identify>	1 Custom Code Required	Vendor Comments
12.0	**Training and Assessment**						
12.1	Live and recorded training sessions		4				Kapstone will provide required trainings
12.2	Task based implementation notes		4				Kapstone will provide required trainings
12.3	Learning material for Platform Implementation and Support		4				Kapstone will provide required trainings
12.4	Assessment criteria for agency shared admin staff for Central platform support and maintenance		4				Kapstone will provide required trainings

EXHIBIT 5

Minority and Women Owned Business Enterprise Commitment

OFFICE OF CONTRACT COMPLIANCE
Nicole Mandeville
DIRECTOR
161 N. Clark Street, Suite 2300 ● Chicago, Illinois 60601 ● (312) 603-5502

January 11, 2024

Mr. Raffi Sarrafian
Chief Procurement Officer
161 North Clark Street – Suite 2300
Chicago, IL 60601

Re: Contract No.: 2112-18598
Enterprise Identity and Access Management (IAM) Implementation
Bureau of Technology (BOT)

Dear Mr. Sarrafian:
The following bid for the above-referenced contract has been reviewed for compliance with the Minority-and Women-owned Business Enterprises (MBE/WBE) Ordinance and have been found to be responsive to the ordinance.

Contractor: Kapstone Technologies LLC DBA Kapstone LLC
Contract Value: $9,680,967.00
Contract Goal: 35% MWBE Direct Participation
Anticipated Term: Sixty (60) months – March 4, 2024 – March 3, 2029
Competitive Bid – Professional Services

MWBE Firm	**Status**	**Certifying Agency**	**Commitment (Direct)**	
Krasan Consulting Services Inc.	WBE - AAPI F	City of Chicago	30%	$2,904,290.00
TeQuity Partners LLC	MBE - AA M	Cook County	5%	$484.048.00
		MWBE Total	**35%**	**$3,388,338.00**

The Office of Contract Compliance has been advised by the Requesting Department that no other bidders are being recommended for award. Original MWBE forms were used in the determination of the responsiveness of this contract.

Sincerely,

JEANETTA CARDINE
Jeanetta Cardine
Contract Compliance Deputy Director

cc: Yaneth Lopez, OCPO
Hema Sundaram, BOT

JC/db

CONTRACT NO. 2112-18598

MBE/WBE UTILIZATION PLAN - FORM 1

BIDDER/PROPOSER HEREBY STATES that all MBE/WBE firms included in this Plan are certified MBEs/WBEs by at least one of the entities listed in the General Conditions – Section 19.

I. BIDDER/PROPOSER MBE/WBE STATUS: (check the appropriate line)

____ Bidder/Proposer is a certified MBE or WBE firm. (If so, attach copy of current Letter of Certification)

____ Bidder/Proposer is a Joint Venture and one or more Joint Venture partners are certified MBEs or WBEs. (If so, attach copies of Letter(s) of Certification, a copy of Joint Venture Agreement clearly describing the role of the MBE/WBE firm(s) and its ownership interest in the Joint Venture and a completed Joint Venture Affidavit – available online at www.cookcountyil.gov/contractcompliance)

✓ Bidder/Proposer is not a certified MBE or WBE firm, nor a Joint Venture with MBE/WBE partners, but will utilize MBE and WBE firms either directly or indirectly in the performance of the Contract. (If so, complete Sections II below and the Letter(s) of Intent – Form 2).

II. ☑ **Direct Participation of MBE/WBE Firms** □ **Indirect Participation of MBE/WBE Firms**

NOTE: Where goals have not been achieved through direct participation, Bidder/Proposer shall include documentation outlining efforts to achieve Direct Participation at the time of Bid/Proposal submission. Indirect Participation will only be considered after all efforts to achieve Direct Participation have been exhausted. Only after written documentation of Good Faith Efforts is received will Indirect Participation be considered.

MBEs/WBEs that will perform as subcontractors/suppliers/consultants include the following:

MBE/WBE Firm: Krasan Consulting Services Inc

Address: 3049 Burlington Ave, Lisle, Illinois-60532

E-mail: Sales@krasanconsulting.com

Contact Person: Pavithra Karumuri Phone: 630-235-8456

Dollar Amount Participation: $ 2,904,290.00

Percent Amount of Participation: 30 %

*Letter of Intent attached? Yes ✓ No _______
*Current Letter of Certification attached? Yes ✓ No _______

MBE/WBE Firm: TeQuity Partners LLC

Address: 3348 S. Prairie Avenue, Chicago, IL 60616

E-mail: mweems@tequitypartners.net

Contact Person: Malcolm Weems Phone: 773-294-4781

Dollar Amount Participation: $ 484,048.00

Percent Amount of Participation: 5 %

*Letter of Intent attached? Yes ✓ No _______
*Current Letter of Certification attached? Yes ✓ No _______

Attach additional sheets as needed.

*** Letter(s) of Intent and current Letters of Certification must be submitted at the time of bid.**

Contract No. 2112-18598

MBE/WBE LETTER OF INTENT - FORM 2

M/WBE Firm: Tequity Partners LLC

Contact Person: Malcolm Weems

Address: 3348 S. Prairie

City/State: Chicago, IL Zip: 60616

Phone: 773-294-4781 Fax: ______

Email: mweems@tequitypartners.net

Certifying Agency: Cook County

Certification Expiration Date: ______

Ethnicity: African-American

Bid/Proposal/Contract #: 2112-18598

FEIN #: 84-4790748

Participation: ☑ Direct □ Indirect

Will the M/WBE firm be subcontracting any of the goods or services of this contract to another firm?

☑ No □ Yes – Please attach explanation. Proposed Subcontractor(s): ______

The undersigned M/WBE is prepared to provide the following Commodities/Services for the above named Project/ Contract: *(If more space is needed to fully describe M/WBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)*

Tequity Partners provides Cisco ISE resources needed for Enterprise Identity and Access Management (IAM) implementation .

Indicate the **Dollar Amount**, **Percentage**, and the **Terms of Payment** for the above-described Commodities/ Services:

5%, payment terms- Net 30

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement for the above work, conditioned upon (1) the Bidder/Proposer's receipt of a signed contract from the County of Cook; (2) Undersigned Subcontractor remaining compliant with all relevant credentials, codes, ordinances and statutes required by Contractor, Cook County, and the State to participate as a MBE/WBE firm for the above work. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/ Supply and Fee/Cost were completed.

Signature (*M/WBE*)	Signature (*Prime Bidder/Proposer*)
Malcolm Weems	Harish Jangada
Print Name	Print Name
Tequity Partners	Kapstone LLC
Firm Name	Firm Name
1/9/2024	01/10/2024
Date	Date
Subscribed and sworn before me	Subscribed and sworn before me
this 9 day of Jan, 2024	this 10 day of January, 2024
Notary Public	Notary Public
"OFFICIAL SEAL" SEAL MADELINE R. ARROYO Notary Public, State of Illinois My Commission Expires April 06, 2024 Commission No. 768270	COLIN ROBINSON SEAL Notary Public - State of New Jersey My Commission Expires May 27, 2026

CONTRACT NO. 2112-18598

MBE/WBE LETTER OF INTENT - FORM 2

M/WBE Firm: Krasan Consulting Services Inc

Contact Person: Pavithra Karumuri

Address: 3049 Burlington Ave.

City/State: Lisle, IL Zip: 60532

Phone: 630-470-4192 Fax: 630 447 0040

Email: sales@krasanconsulting.com

Certifying Agency: City of Chicago-Department of Procurement Services

Certification Expiration Date: July 15, 2024

Ethnicity: Asian

Bid/Proposal/Contract #: 2112-18598

FEIN #: 82-5263603

Participation: [✓] Direct [ ] Indirect

Will the M/WBE firm be subcontracting any of the goods or services of this contract to another firm?

[✓] No [ ] Yes – Please attach explanation. Proposed Subcontractor(s): ____________________

The undersigned M/WBE is prepared to provide the following Commodities/Services for the above named Project/ Contract: *(If more space is needed to fully describe M/WBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)*

General Consulting Services, IT consulting, Implementation

Indicate the **Dollar Amount**, **Percentage**, and the **Terms of Payment** for the above-described Commodities/ Services:

Dollar amount- TBD, Percentage-30%, Terms of Payment-Net 30.

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement for the above work, conditioned upon (1) the Bidder/Proposer's receipt of a signed contract from the County of Cook; (2) Undersigned Subcontractor remaining compliant with all relevant credentials, codes, ordinances and statutes required by Contractor, Cook County, and the State to participate as a MBE/WBE firm for the above work. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/ Supply and Fee/Cost were completed.

Signature (*M/WBE*)

Pavithra Karumuri
Print Name

Krasan Consulting Services Inc
Firm Name

01/08/2024
Date

Subscribed and sworn before me

this 8 day of January, 2024

Notary Public Samantha Stanciu

SEAL

SAMANTHA STANCIU
Official Seal
Notary Public - State of Illinois
My Commission Expires Apr 15, 2026

Signature (*Prime Bidder/Proposer*)

Harish Jangada
Print Name

Kapstone LLC
Firm Name

01/10/2024
Date

Subscribed and sworn before me

this 10th day of January, 2024.

Notary Public

SEAL

COLIN ROBINSON
Notary Public - State of New Jersey
My Commission Expires May 27, 2026

PETITION FOR WAIVER OF MBE/WBE PARTICIPATION – FORM 3

A. BIDDER/PROPOSER HEREBY REQUESTS:

□ FULL MBE WAIVER □ FULL WBE WAIVER

□ REDUCTION (PARTIAL MBE and/or WBE PARTICIPATION)

_____% of Reduction for MBE Participation
_____% of Reduction for WBE Participation

N/A

B. REASON FOR FULL/REDUCTION WAIVER REQUEST

Bidder/Proposer shall check each item applicable to its reason for a waiver request. Additionally, supporting documentation shall be submitted with this request.

□ (1) Lack of sufficient qualified MBEs and/or WBEs capable of providing the goods or services required by the contract. **(Please explain)**

□ (2) The specifications and necessary requirements for performing the contract make it impossible or economically infeasible to divide the contract to enable the contractor to utilize MBEs and/or WBEs in accordance with the applicable participation. **(Please explain)**

□ (3) Price(s) quoted by potential MBEs and/or WBEs are above competitive levels and increase cost of doing business and would make acceptance of such MBE and/or WBE bid economically impracticable, taking into consideration the percentage of total contract price represented by such MBE and/or WBE bid. **(Please explain)**

□ (4) There are other relevant factors making it impossible or economically infeasible to utilize MBE and/or WBE firms. **(Please explain)**

N/A

C. GOOD FAITH EFFORTS TO OBTAIN MBE/WBE PARTICIPATION

□ (1) Made timely written solicitation to identified MBEs and WBEs for utilization of goods and/or services; and provided MBEs and WBEs with a timely opportunity to review and obtain relevant specifications, terms and conditions of the proposal to enable MBEs and WBEs to prepare an informed response to solicitation. **(Attach of copy written solicitations made)**

□ (2) Used the services and assistance of the Office of Contract Compliance staff. **(Please explain)**

□ (3) Timely notified and used the services and assistance of community, minority and women business organizations. **(Attach of copy written solicitations made)**

□ (4) Followed up on initial solicitation of MBEs and WBEs to determine if firms are interested in doing business. **(Attach supporting documentation)**

☒ (5) Engaged MBEs & WBEs for direct/indirect participation. **(Please explain)**

D. OTHER RELEVANT INFORMATION

Attach any other documentation relative to Good Faith Efforts in complying with MBE/WBE participation.

I. POLICY AND GOALS

A. It is the policy of the County of Cook to prevent discrimination in the award of or participation in County Contracts and to eliminate arbitrary barriers for participation in such Contracts by local businesses certified as a Minority Business Enterprise (MBE) and Women-owned Business Enterprise (WBE) as both prime and sub-contractors. In furtherance of this policy, the Cook County Board of Commissioners has adopted a Minority- and Women-owned Business Enterprise Ordinance (the "Ordinance") which establishes annual goals for MBE and WBE participation as outlined below:

Contract Type	**Goals**	
	MBE	**WBE**
Goods and Services	25%	10%
Construction	24%	10%
Professional Services	35% Overall	

B. **The County shall set contract-specific goals, based on the availability of MBEs and WBEs that are certified to provide commodities or services specified in this solicitation document. The MBE/WBE participation goals for this Agreement is [thirty-five percent (35%)].** A Bid, Quotation, or Proposal shall be rejected if the County determines that it fails to comply with this General Condition in any way, including but not limited to: (i) failing to state an enforceable commitment to achieve for this contract the identified MBE/WBE Contract goals; or (ii) failing to include a Petition for Reduction/Waiver, which states that the goals for MBE/WBE participation are not attainable despite the Bidder or Proposer Good Faith Efforts, and explains why. If a Bid, Quotation, or Proposal is rejected, then a new Bid, Quotation, or Proposal may be solicited if the public interest is served thereby.

C. To the extent that a Bid, Quotation, or Proposal includes a Petition for Reduction/Waiver that is approved by the Office of Contract Compliance, the Contract specific MBE and WBE participation goals may be achieved by the proposed Bidder or Proposer's status as an MBE or WBE; by the Bidder or Proposer's enforceable joint-venture agreement with one or more MBEs and/or WBEs; by the Bidder or Proposer entering into one or more enforceable subcontracting agreements with one or more MBE and WBE; by the Bidder or Proposer establishing and carrying out an enforceable mentor/protégé agreement with one or more MBE and WBE; by the Bidder or Proposer actively engaging the Indirect Participation of one or more MBE and WBE in other aspects of its business; or by any combination of the foregoing, so long as the Utilization Plan evidences a commitment to meet the MBE and WBE Contract goals set forth in (B) above, as approved by the Office of Contract Compliance.

D. A single Person, as defined in the Procurement Code, may not be utilized as both an MBE and a WBE on the same Contract, whether as a Consultant, Subcontractor or supplier.

E. Unless specifically waived in the Bid or Proposal Documents, this Exhibit; the Ordinance; and the policies and procedures promulgated thereunder shall govern. If there is a conflict between this Exhibit and the Ordinance or the policies and procedures, the Ordinance shall control.

F. A Consultant's failure to carry out its commitment regarding MBE and WBE participation in the course of the Contract's performance may constitute a material breach of the Contract. If such breach is not appropriately cured, it may result in withholding of payments under the Contract, contractual penalties, disqualification and any other remedy provided for in Division 4 of the Procurement Code at law or in equity.

II. REQUIRED BID OR PROPOSAL SUBMITTALS

A Bidder or Proposer shall document its commitment to meeting the Contract specific MBE and WBE participation goals by submitting a Utilization Plan with the Bid or Proposal. The Utilization Plan shall include (1) one or more Letter(s) of Intent from the relevant MBE and WBE firms; and (2) current Letters of Certification as an MBE or WBE. Alternatively, the Bidder or Proposer shall submit (1) a written Petition for Reduction/Waiver with the Bid, Quotation or Proposal, which documents its preceding Good Faith Efforts and an explanation of its inability to meet the goals for MBE and WBE participation. The Utilization Plan shall be submitted at the time that the bid or proposal is due. **Failure to include a Utilization Plan will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

A. MBE/WBE Utilization Plan

Each Bid or Proposal shall include a complete Utilization Plan, as set forth on Form 1 of the M/WBE Compliance Forms. The Utilization Plan shall include the name(s), mailing address, email address, and telephone number of the principal contact person of the relevant MBE and WBE firms. If the Bidder or Proposer submits a Bid or Proposal, and any of their subconsultants, suppliers or consultants, are certified MBE or WBE firms, they shall be identified as an MBE or WBE within the Utilization Plan.

1. Letter(s) of Intent

Except as set forth below, a Bid or Proposal shall include, as part of the Utilization Plan, one or more Letter(s) of Intent, as set forth on Form 2 of the M/WBE Compliance Forms, executed by each MBE and WBE and the Bidder or Proposer. The Letter(s) of Intent will be used to confirm that each MBE and WBE shall perform work as a Subcontractor, supplier, joint venture, or consultant on the Contract. Each Letter of Intent shall indicate whether and the degree to which the MBE or WBE will provide goods or services directly or indirectly during the term of the Contract. The box for direct participation shall be marked if the proposed MBE or WBE will provide goods or services directly related to the scope of the Contract. The box for Indirect participation shall be marked if the proposed MBE or WBE will not be directly involved in the Contract but will be utilized by the Bidder or Proposer for other services not related to the Contract. Indirect Participation shall not be counted toward the participation goal. Each Letter of Intent shall accurately detail the work to be performed by the relevant MBE or WBE firm, the agreed dollar amount, the percentage of work, and the terms of payment.

Failure to include Letter(s) of Intent will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

All Bids and Proposals must conform to the commitments made in the corresponding Letter(s) of Intent, as may be amended through change orders.

The Contract Compliance Director may at any time request supplemental information regarding Letter(s) of Intent, and such information shall be furnished if the corresponding Bid or Proposal is to be deemed responsive.

2. Letter(s) of Certification

Only current Letter(s) of Certification from one of the following entities may be accepted as proof of certification for MBE/WBE status, provided that Cook County's requirements for certification are met:

- County of Cook
- City of Chicago

Persons that are currently certified by the City of Chicago in any area other than Construction/Public Works shall also complete and submit a MBE/WBE Reciprocal Certification Affidavit along with a current letter of certification from the City of Chicago. This Affidavit form can be downloaded from www.cookcountyil.gov/contractcompliance.

The Contract Compliance Director may reject the certification of any MBE or WBE on the ground that it does not meet the requirements of the Ordinance, or the policies and rules promulgated thereunder.

3. Joint Venture Affidavit

In the event a Bid or Proposal achieves MBE and/or WBE participation through a Joint Venture, the Bid or Proposal shall include the required Joint Venture Affidavit, which can be downloaded from www.cookcountyil.gov/contractcompliance. The Joint Venture Affidavit shall be submitted with the Bid or Proposal, along with current Letter(s) of Certification.

B. Petition for Reduction/Waiver

In the event a Bid or Proposal does not meet the Contract specific goals for MBE and WBE participation, the Bid or Proposal shall include a Petition for Reduction/Waiver, as set forth on Form 3. The Petition for Reduction/Waiver shall be supported by sufficient evidence and documentation to demonstrate the Bidder or Proposer's Good Faith Efforts in attempting to achieve the applicable MBE and WBE goals, and its inability to do so despite its Good Faith Efforts.

Failure to include Petition for Reduction/Waiver will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

III. REDUCTION/WAIVER OF MBE/WBE GOALS

A. Granting or Denying a Reduction/Waiver Request.

1. The adequacy of the Good Faith Efforts to utilize MBE and WBE firms in a Bid or Proposal will be evaluated by the CCD under such conditions as are set forth in the Ordinance, the policies and rules promulgated thereunder, and in the "Petition for Reduction/Waiver of MBE/WBE Participation Goals" – Form 3 of the M/WBE Compliance Forms.

2. With respect to a Petition for Reduction/Waiver, the sufficiency or insufficiency of a Bidder or Proposer's Good Faith Efforts shall be evaluated by the CCD as of the date upon which the corresponding Bid or Proposal was due.

3. The Contract Compliance Director or his or her duly authorized Waiver Committee may grant or deny the Petition for Reduction/Waiver based upon factors including but not limited to: (a) whether sufficient qualified MBE and WBE firms are unavailable despite good faith efforts on the part of the Bidder or Proposer; (b) the degree to which specifications and the reasonable and necessary requirements for performing the Contract make it impossible or economically infeasible to divide the Contract into sufficiently small tasks or quantities so as to enable the Bidder or Proposer to utilize MBE and WBE firms in accordance with the applicable goals; (c) the degree to which the prices or prices required by any potential MBE or WBE are more that 10% above competitive levels; and (d) such other factors as are determined relevant by the Contract Compliance Director or the duly authorized Waiver Committee.

4. If the Contract Compliance Director or the duly authorized Waiver Committee determines that the Bidder or Proposer has not demonstrated sufficient Good Faith Efforts to meet the applicable MBE and WBE goals, the Contract Compliance Director or the duly authorized Waiver Committee may deny a Petition for Reduction/Waiver, declare the Bid or Proposal non-responsive, and recommend rejection of the Bid, Quotation, or Proposal.

IV. CHANGES IN CONSULTANT'S UTILIZATION PLAN

A. A Consultant, during its performance of the Contract, may not change the original MBE or WBE commitments specified in the relevant Utilization Plan, including but not limited to, terminating a MBE or WBE Contract, reducing the scope of the work to be performed by a MBE/WBE, or decreasing the price to a MBE/WBE, except as otherwise provided by the Ordinance and according to the policies and procedures promulgated thereunder.

B. Where a Person listed under the Contract was previously considered to be a MBE or WBE but is later found not to be, or work is found not to be creditable toward the MBE or WBE goals as stated in the Utilization Plan, the Consultant shall seek to discharge the disqualified enterprise, upon proper written notification to the Contract Compliance Director, and make every effort to identify and engage a qualified MBE or WBE as its replacement. Failure to obtain an MBE or WBE replacement within 30 business days of the Contract Compliance Director's written approval of the removal of a purported MBE or WBE may result in the termination of the Contract or the imposition of such remedy authorized by the Ordinance, unless a written Petition for Reduction/Waiver is granted allowing the Consultant to award the work to a Person that is not certified as an MBE or WBE.

V. NON-COMPLIANCE

If the CCD determines that the Consultant has failed to comply with its contractual commitments or any portion of the Ordinance, the policies and procedures promulgated thereunder, or this Exhibit, the Contract Compliance Director shall notify the Consultant of such determination and may take any and all appropriate actions as set forth in the Ordinance or the policies and procedures promulgated thereunder which includes but is not limited to disqualification, penalties, withholding of payments or other remedies in law or equity.

VI. REPORTING/RECORD-KEEPING REQUIREMENTS

The Consultant shall comply with the reporting and record-keeping requirements in the manner and time established by the Ordinance, the policies and procedure promulgated thereunder, and the Contract Compliance Director. Failure to comply with such reporting and record-keeping requirements may result in a declaration of Contract default. Upon award of a Contract, a Consultant shall acquire and utilize all Cook County reporting and record-keeping forms and methods which are made available by the Office of Contract Compliance. MBE and WBE firms shall be required to verify payments made by and received from the prime Consultant.

VII. EQUAL EMPLOYMENT OPPORTUNITY

Compliance with MBE and WBE requirements will not diminish or supplant other legal Equal Employment Opportunity and Civil Rights requirements that relate to Consultant and Subcontractor obligations.

Any questions regarding this section should be directed to:
Contract Compliance Director
Cook County Office of Contract Compliance
161 N. Clark Street, Suite 2300
Chicago, Illinois 60601
(312) 603-5502

EXHIBIT 6

Evidence of Insurance

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
1/9/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Hugh Wood Inc, Philadelphia
200 South Broad Street
Philadelphia PA 19102

CONTACT NAME:
PHONE (A/C, No, Ext): 215-732-0500 **FAX (A/C, No):** 215-732-1208
E-MAIL ADDRESS: insurance@hughwood.com

INSURED ICCONSU-01
Kapstone Technologies LLC;
iC Consult Group Americas Corp.
271 17th Street NW, Ste 1750
Atlanta GA 30363

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Hartford Fire Insurance Co	19682
INSURER B : Trumbull Insurance Co.	
INSURER C : Hartford Casualty Insurance Co	29424
INSURER D : Princeton Excess & Surplus	
INSURER E : Scottdale Indemnity Company	15580
INSURER F :	

COVERAGES CERTIFICATE NUMBER: 252576262 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY	Y		39UUNDQ0199	1/10/2024	1/10/2025	EACH OCCURRENCE	$ 1,000,000
	□ □ CLAIMS-MADE ☒ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 300,000
	□						MED EXP (Any one person)	$ 10,000
	□						PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	☒ POLICY □ PRO-JECT □ LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
B	AUTOMOBILE LIABILITY	Y		39UENDQ0569	1/10/2024	1/10/2025	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	□ ANY AUTO						BODILY INJURY (Per person)	$
	□ OWNED AUTOS ONLY □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
	□ □							$
C	☒ UMBRELLA LIAB ☒ OCCUR			39XHUDO1671	1/10/2024	1/10/2025	EACH OCCURRENCE	$ 3,000,000
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	$ 3,000,000
	DED ☒ RETENTION $ 10,000							$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N						PER STATUTE OTH-ER	
	ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBEREXCLUDED? □	N / A					E.L. EACH ACCIDENT	$
	(Mandatory in NH)						E.L. DISEASE - EA EMPLOYEE	$
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - POLICY LIMIT	$
D E	Tech E&O/Cyber Liability XS Tech E&O/Cyber Liability			5DA3CY0000236-02 EKI3484821	6/30/2023 6/30/2023	6/30/2024 6/30/2024	Each Claim Each Claim	2,500,000 2,500,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Additional Named Insureds:
Kapstone Technologies LLC
iCSynergy International, LLC
SecureITSource, Inc.
iC Consult Americas, LLC
Cook County Government is included as Additional Insured with respects to the General Liability and Business Auto Liability as required by written contract.

CERTIFICATE HOLDER

Cook County Government
161 N. Clark Street, Suite 2300
Chicago IL 60601

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
Simon Codrington

EXHIBIT 7

Board Authorization

Board of Commissioners of Cook County

118 North Clark Street
Chicago, IL

NEW CONTRACT #2112-18598
approved at 02/29/24 Board

Legislation Details (With Text)

File #:	24-0883 **Version:** 1	**Name:**	KapStone Contract 2024
Type:	Contract (Technology)	**Status:**	Approved
File created:	1/2/2024	**In control:**	Technology and Innovation Committee
On agenda:	1/25/2024	**Final action:**	2/29/2024

Title: PROPOSED CONTRACT (TECHNOLOGY)

Department(s): Bureau of Technology

Vendor: Kapstone Technologies LLC dba Kapstone, LLC, Somerset, New Jersey

Request: Authorization for the Chief Procurement Officer to enter into and execute contract

Good(s) or Service(s): Enterprise Identity and Access Management (IAM) Software

Contract Value: $9,680,967.00

Contract period: 3/4/2024 - 3/3/2029 with two (2) one-year renewal options

Potential Fiscal Year Budget Impact: FY 2024-$2,606,000.00; FY 2025-$3,622,622.00; FY 26-$1,582,345.00; FY 27-$935,000.00; FY 2028-$935,000.00

Accounts: 11569.1009.21120.560225.00000.00000

Contract Number(s): 2112-18598

Concurrence(s):
The vendor has met the Minority- and Women-owned Business Enterprise Ordinance via: Direct participation.

The Chief Procurement Officer concurs.

TECHNOLOGY: N/A

Summary: Identity Access Management is a fundamental component of the County's IT strategy to ensure security, efficiency, and compliance with IT operations. It contributes to cost efficiency by automating user provisioning and de-provisioning processes. This reduces the administrative overhead associated with managing user access and helps organizations optimize their IT resources.

This contract is awarded through Request for Proposals (RFP) procedures in accordance with Cook County Procurement Code. Kapstone, LLC was selected based on established evaluation criteria.

Sponsors:

Indexes: F. THOMAS LYNCH, Chief Information Officer, Bureau of Technology

Code sections:

Attachments:

Date	Ver.	Action By	Action	Result
2/29/2024	1	Board of Commissioners	approve	Pass
1/25/2024	1	Board of Commissioners	refer	Pass

PROPOSED CONTRACT (TECHNOLOGY)

Department(s): Bureau of Technology

Vendor: Kapstone Technologies LLC dba Kapstone, LLC, Somerset, New Jersey

Request: Authorization for the Chief Procurement Officer to enter into and execute contract

Good(s) or Service(s): Enterprise Identity and Access Management (IAM) Software

Contract Value: $9,680,967.00

Contract period: 3/4/2024 - 3/3/2029 with two (2) one-year renewal options

Potential Fiscal Year Budget Impact: FY 2024-$2,606,000.00; FY 2025-$3,622,622.00; FY 26-$1,582,345.00; FY 27-$935,000.00; FY 2028-$935,000.00

Accounts: 11569.1009.21120.560225.00000.00000

Contract Number(s): 2112-18598

Concurrence(s):
The vendor has met the Minority- and Women-owned Business Enterprise Ordinance via: Direct participation.

The Chief Procurement Officer concurs.

TECHNOLOGY: N/A

Summary: Identity Access Management is a fundamental component of the County’s IT strategy to ensure security, efficiency, and compliance with IT operations. It contributes to cost efficiency by automating user provisioning and de-provisioning processes. This reduces the administrative overhead associated with managing user access and helps organizations optimize their IT resources.

This contract is awarded through Request for Proposals (RFP) procedures in accordance with Cook County Procurement Code. Kapstone, LLC was selected based on established evaluation criteria.

EXHIBIT 8

Identification of Subcontractor/Supplier/Subconsultant Form

Contract #: 2112-18598

OCPO ONLY:
☒ Disqualification Check Complete

Cook County
Office of the Chief Procurement Officer
Identification of Subcontractor/Supplier/Subconsultant Form

The Bidder/Proposer/Respondent (“the Contractor”) will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form (“ISF”) with each Bid, Request for Proposal, and Request for Qualification. **The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract**. In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

Bid/RFP/RFQ No.: 2112-18598	Date: 9/26/2022
Total Bid or Proposal Amount: **$9,680,967.00**	Contract Title: Enterprise Identity and Access Management (IAM)
Contractor: Kapstone Technologies LLC DBA Kapstone Ll	Subcontractor/Supplier/ Subconsultant to be added or substitute: Krasan Consulting Services Inc
Authorized Contact for Contractor: Harish Jangada	Authorized Contact for Subcontractor/Supplier/ Subconsultant: Pavithra Karumuri
Email Address (Contractor): harish.jangada@kapstonellc.com	Email Address (Subcontractor): Sales@krasanconsulting.com
Company Address (Contractor): 370 Campus Drive # 108	Company Address (Subcontractor): 3049 Burlington Ave
City, State and Zip (Contractor): Somerset, NJ - 08873	City, State and Zip (Subcontractor): Lisle, Illinois-60532
Telephone and Fax (Contractor): 732 356 5130	Telephone and Fax (Subcontractor): 630-235-8456 and Fax number- 630 447 004(
Estimated Start and Completion Dates (Contractor): Based on the contract Award date	Estimated Start and Completion Dates (Subcontractor): At the kick-off of the project, If contract is awa

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

Description of Services or Supplies	**Total Price of Subcontract for Services or Supplies**
Consulting Services	$ 2,904,290.00

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. **This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract’s approved MBE/WBE/Utilization Plan must be submitted to the Office of the Contract Compliance.**

Kapstone Technologies LLC DBA Kapstone LLC
Contractor

Harish Jangada
Name

CEO
Title

Jangada 01/03/2024
Prime Contractor Signature Date

OCPO ONLY:
□ Disqualification
☒ Check Complete

Cook County
Office of the Chief Procurement Officer
Identification of Subcontractor/Supplier/Subconsultant Form

The Bidder/Proposer/Respondent ("the Contractor") will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form ("ISF") with each Bid, Request for Proposal, and Request for Qualification. **The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract**. In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

Bid/RFP/RFQ No.: 2112-18598	Date: 01/03/2024
Total Bid or Proposal Amount: $9,680,967.00	Contract Title: Enterprise Identity and Access Management (IAM)
Contractor: Kapstone Technologies LLC DBA Kapstone Ll	Subcontractor/Supplier/ Subconsultant to be added or substitute: TeQuity Partners LLC
Authorized Contact for Contractor: Harish Jangada	Authorized Contact for Subcontractor/Supplier/ Subconsultant: Malcolm Weems
Email Address (Contractor): harish.jangada@kapstonellc.com	Email Address (Subcontractor): mweems@tequitypartners.net
Company Address (Contractor): 370 Campus Drive #108	Company Address (Subcontractor): 3348 S. Prairie Avenue
City, State and Zip (Contractor): Somerset, NJ - 08873	City, State and Zip (Subcontractor): Chicago, IL 60616
Telephone and Fax (Contractor): 732 356 5130	Telephone and Fax (Subcontractor): 773-294-4781
Estimated Start and Completion Dates (Contractor): TBD	Estimated Start and Completion Dates (Subcontractor): TeQuity will be proviidng CISCO ISE services

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

Description of Services or Supplies	**Total Price of Subcontract for Services or Supplies**
Providing Cisco ISE resources	$484,048.00

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. **This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract's approved MBE/WBE/Utilization Plan must be submitted to the Office of the Contract Compliance.**

Kapstone Technologies LLC DBA Kapstone LLC
Contractor

Harish Jangada
Name

CEO
Title

Jangada
Prime Contractor Signature

01/03/2024
Date

EXHIBIT 9

Electronic Payables Program

OFFICE OF THE COOK COUNTY COMPTROLLER
ELECTRONIC PAYABLES PROGRAM ("E-PAYABLES")

FOR INFORMATION PURPOSES ONLY

This document describes the Office of the Cook County Comptroller's Electronic Payables Program ("E-Payables").
If you wish to participate in E-Payables, please contact the Cook County Comptroller's Office, Accounts Payable, 161 N. Clark Street, Suite 1900, Chicago, IL 60601.

DESCRIPTION

To increase payment efficiency and timeliness, we have introduced E-Payables program, a new payment initiative to our accounts payable model. This new initiative utilizes a Visa purchasing card and operates through the Visa payment network. This is County's preferred method of payment and your participation in our Visa purchasing card program will provide mutual benefits both to your organization and ours.

As a vendor, you may experience the following benefits by accepting this new payment type:

- Improved cash flow and accelerated payment
- Reduced paperwork and a more streamlined accounts receivable process
- Elimination of stop payment issues
- Reduced payment delays
- Reduced costs for handling paper checks
- Payments settled directly to your merchant account

There are two options within this initiative:

3. Dedicated Credit Card – "PULL" Settlement

For this option, you will have an assigned dedicated credit card to be used for each payment. You will provide a point of contact within your organization who will keep credit card information on file. Each time a payment is made, you will receive a remittance advice via email detailing the invoices being paid. Each time you receive a remittance advice, you will process payments in the same manner you process credit card transactions today.

4. One-Time Use Credit Card – "SUGA" Settlement

For this option, you will provide a point of contact within your organization who will receive an email notification authorizing you to process payments in the same manner you process credit card transactions today. Each time payment is made, you will receive a remittance advice, via email, detailing the invoices being paid. Also, each time you receive a remittance advice, you will receive a new, unique credit card number. This option is ideal for suppliers who are unable to keep credit card account information on file.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 10

Cook County Travel Policy

COOK COUNTY BUREAU OF FINANCE		
POLICY TITLE: EMPLOYEE AND OFFICIAL BUSINESS AND TRAVEL EXPENSE REIMBURSEMENT POLICY		**Applicable Forms may be found at:** https://www.cookcountyil.gov/service/travel-and-business-expenses-policy-and-procedures
Effective: July 15, 2023	**Supersedes: FY2017**	**Page 1 of 21**

I. GENERAL PROVISIONS

A. Overview

Applicable law provides that Employees and Officials are entitled to reimbursement for certain business and travel expenses.[1] This policy sets forth the business and travel expense reimbursement policy for the County of Cook ("County"), and it establishes guidelines for the reimbursement of authorized and Necessary Business Expenses incurred on behalf of the County. The County will not reimburse Employees and Officials for expenditures that do not comply with the provisions of this policy.

B. Purpose

The purpose of this policy is to provide guidelines for the payment of authorized and Necessary Business Expenses that cannot be obtained using the methods provided in the Cook County Procurement Code, and to enable Employees and Officials to successfully execute their Local and Non-local travel requirements at the lowest reasonable costs, resulting in the best value for the County. The Chief Financial Officer (or designee) may be contacted for clarification as needed.

C. Intent

This policy is intended to be interpreted consistent with and subject to applicable law and other related County policies. *See* Related Policies below. It supersedes all previous policies and/or memoranda that may have been issued from time to time on subjects covered in this policy or other policies that may contain provisions related to reimbursement for business and travel expenses. This policy is not intended for tuition reimbursement. See Related Policies. This policy is not intended to supersede or limit the County from enforcing programs or provisions in any applicable collective bargaining agreement.

D. Severability

If any section or provision of this document should be held invalid by operation of law, none of the remainder shall be affected.

[1] *See* Illinois Wage Payment and Collection Act, 820 ILCS 115/9.5.

E. **Jurisdiction**

The Cook County Chief Financial Officer, in consultation with the Director of Budget and Management Services ("Budget") and the Comptroller are authorized to develop and issue policies and procedures for business and travel expense reimbursement.

F. **Areas Affected**

This policy and the procedures associated with this policy applies to all elected and appointed Officials and Employees in departments, offices, institutions or agencies of the County, including but not limited to the offices and departments under the jurisdiction of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System ("CCH"), Cook County State's Attorney, Cook County Sheriff, Cook County Public Defender, Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, the Office of the Independent Inspector General, the Cook County Land Bank Authority ("Land Bank Authority"), and the Public Administrator (hereinafter, "Agencies" or "Agency") who incur Necessary Business Expenses while conducting official business on behalf of the County.

G. **Nondiscrimination**

Cook County prohibits the discriminatory application, implementation, or enforcement of any provision of this policy based on race, color, sex, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military discharge status, source of income, gender identity or housing status, or any other protected category established by law, statute, or ordinance.

H. **Definitions**

For purposes of this policy, the following terms shall be given the following meanings as set forth below:

Affidavit for Lost Receipts means the form submitted by the Employee or Official to request reimbursement of eligible Necessary Business Expenses when itemized receipts or other proof of expense and payment is not available due to being lost or stolen.

Agency or Agencies means offices and departments under the jurisdiction of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System, Cook County State's Attorney, Cook County Sheriff, Cook County Public Defender, Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, the Office of the Independent Inspector General, the Cook County Land Bank Authority, and the Public Administrator.

Alternative Worksite means an employee's work location other than the County employee's Official Worksite. This definition may include an Employee or Official's residence when telecommuting or may include the location of a field assignment or 3rd party meeting in certain circumstances.

Appropriate Authorizing Party (or designee) means the Employee or Official authorized to commit County resources and to preapprove expenses for purposes of reimbursement and to approve reimbursements under this policy, per section (J)(1)(c) below.

Appropriated Funds or Funding means money allocated by legislation passed by the Cook County Board of Commissioners and signed by the President of the Board of Commissioners, whether from an annual appropriation, multi-year appropriation, appropriated user fee, mandatory appropriation, or reimbursements from such appropriations, etc.

Business and/or Travel Expense Reimbursement Form means the reimbursement form submitted by the Employee or Official to the Appropriate Approving Party for authorization of expense reimbursement.

Common carrier means Non-local travel by airplane, train (i.e., Amtrak, or similar), bus (i.e., Greyhound, or similar).

Commuting means travel between the Official's or Employee's residence and the Official's or Employee's Official Worksite.

County means Cook County.

County vehicle means travel by pool fleet or similar.

Employee means an individual employed by an Agency.

Local travel means travel within a 60-mile radius from the Official's or Employee's Official Worksite, for official County business.

Necessary Business Expenses mean authorized out-of-pocket expenses or losses that are incurred by the Official or Employee in the discharge of employment or official duties, that inure to the primary benefit of the County and can't be procured under the County's Procurement Code or Direct Pay Policy. The County will not be responsible for losses or expenses incurred due to an Employee's or Official's own negligence, losses due to normal wear, or losses due to theft unless the theft was due to the County's negligence.

Non-local travel means travel in excess of a 60-mile radius from the Official's or Employee's Official Worksite, for official County business.

Personal leased vehicle means travel by a leased vehicle, or similar, that is not a vehicle that is leased by the County as part of the County's fleet.

Personally owned or Personal vehicle means travel by a vehicle that is personally owned by the Employee, Official, or similar.

Official Worksite means the worksite to which the Official or Employee is typically assigned.

Pre-Authorization Form means the form submitted by the Requester seeking reimbursement for a Necessary Business Expense.

Public transportation means local travel by CTA, Pace, Metra, or similar.

Rental Car means travel by vehicle hired from a car rental agency for a short period of time during Non-local official County business.

Requester means the Employee or Official seeking reimbursement.

Ride share or *ride sharing* means travel by Taxi, Shuttle, Lyft, Uber, Divvy, Zip Car, or similar.

Transportation Expense Voucher means a mileage reimbursement voucher for authorized use of personally owned vehicles in the conduct of official County business.

I. Responsibilities of Employees, Management, and County Officials

Employees and Officials requesting Necessary Business Expense reimbursements are responsible for ensuring that the reimbursement request is truthful and accurate, complies with all applicable policies, is properly authorized before the expense is incurred, and is supported by the required receipts and documentation. Strict conformance with this policy is required to ensure eligibility for reimbursement when incurring expenses on behalf of the County and/or requesting expense reimbursements. Fraudulent or improper submissions for reimbursement may lead to disciplinary action or ethics fines/penalties. In addition, using or attempting to use this expense reimbursement policy when an Employee or Official should be using the Procurement Code process to purchase items or services on behalf of the County may lead to the expense being ineligible for reimbursement.

Moreover, any Employee or Official who receives an unauthorized or an erroneously issued reimbursement payment from the County, must immediately return such payment within thirty (30) days from the time the Employee or Official has become aware of the unauthorized or erroneous reimbursement or notice from the Comptroller's Office or the Budget Office. Failure to comply with this provision will result in disciplinary or other appropriate action depending on the Employee(s) or Officials(s) involved and the specific circumstances. In the event repayment is made by an Employee or Official through payroll deduction, the Comptroller's Office will handle in accordance with its procedures for payroll deductions.

Strict adherence to the County's Code of Ethical Conduct and Office of the Independent Inspector General Ordinance is required. Expenditures that do not comply with the County's Ethics Ordinance or Office of the Independent Inspector General Ordinance and this policy shall be denied and may be referred to the Board of Ethics or Inspector General for investigation. For example, expenditures made in connection with "prohibited political activity," as defined in section 2-562 of the Cook County Code, shall not be reimbursed.

Each Appropriate Authorizing Party is responsible for ensuring that all expenditures made on behalf of the County comply with all applicable policies. Additionally, each Appropriate Authorizing Party is accountable for the appropriate use of County funds and must verify that all Necessary Business Expenses are budgeted and charged to the proper account(s). In addition, before approving any expense reimbursement, the Authorizing Party must ensure that the requesting Employee or Official received pre-authorization to incur the expense where required, the expense is legitimate, properly documented, and, if proper procedures are not followed, not approving the reimbursement request. Failure to adhere to these obligations may result in appropriate corrective action, including but not limited to disciplinary action, depending on the Employees(s) or Official(s) involved and the specific circumstances.

The Chief Financial Officer has designated the Director of Budget and Management Services to monitor County practices to ensure compliance with, and answer questions concerning, the information presented in this policy.

J. Policy and Procedures

1. General. The County has a fiduciary responsibility to ensure County resources are used responsibly and that Employees and Officials do not incur inappropriate or excessive expenses or gain financially from the County. Necessary Business Expenses will be reimbursed in accordance with IRS guidelines and with the provisions of this policy, provided there is sufficient funding for this purpose in the Department's budget and doing so would not circumvent the Cook County Procurement Code. A Necessary Business Expense must have a clear and legitimate business purpose. All out of country travel-related expenditures will conform to the IRS guidelines and the U.S. General Services Administration whenever possible. See, https://www.gsa.gov/travel-resources. Where compliance with IRS and the U.S. General Services Administration guidelines cannot be met, approval of such expense must be documented by the Appropriate Authorizing Party. Excessive costs or unjustifiable costs are not acceptable and will not be reimbursed.

(a) *Appropriated Funding*. Expenditures shall be charged to the appropriate account of the department incurring the expense, as designated in the department's annual appropriation.

(b) *Grant requirements*. Expenditures connected to and/or funded by a grant (or contract) shall be made in accordance with the grantor's requirements, and reimbursement will be made at the rate specified by the grant (or contract), or if no specified rate, at the County's rate defined by this policy.

(c) *Appropriate Authorizing Party.* Necessary Business Expenses using the Pre-Authorization Form must be submitted for pre-authorization to the Requester's:

(1) Department Head, if requested by an Employee within the Department Head's Department except where the Bureau Chief has indicated by internal memo or policy that Bureau Chief approval is required;

(2) Bureau Chief, if requested by a Department Head;

(3) Chief of Staff, if requested by a Bureau Chief;

(4) Employing Official, if requested by a Chief of Staff or

(5) Where there is no person in a higher-level position within the Requester's organizational chart to authorize the expense, such as an Official, the reimbursement request shall be referred to the Agency's Chief of Staff, where applicable or the Budget Director if the Agency does not employ a Chief of Staff for pre-authorization.

Individuals are strictly prohibited from authorizing their own requests to incur and be reimbursed for a Necessary Business Expense. The Appropriate Authorizing Party must confirm there is available funding in the Agency's appropriated annual budget prior to approving the Pre-Authorization Form.

(d) *Tax Exempt Status.* Expenditures must exclude sales tax to the extent permitted under law. Tax exempt certificates may be requested in advance of expenditures through the Office of the Chief Procurement Officer by emailing taxexemptrequest@cookcountyil.gov. Use of vendors who will not accept tax exempt certificates are prohibited absent exigent circumstances.

II. INELIGIBLE EXPENSES

The following expenses are **not** Necessary Business Expenses and shall **not** be reimbursed under this policy:

A. Expenditures made in connection with "prohibited political activity," as defined in section 2-562 of the Cook County Code or that violate the Ethics Code, 2-560 et. seq.;

B. Expenses incurred without proper pre-authorization unless otherwise approved in writing by the Appropriate Authorizing Party;

C. Expenses incurred in excess of the allowable limits in this policy unless otherwise approved in writing by the Appropriate Authorizing Party as set forth herein;

D. Expenses for leasing or purchasing items for workspace/office, such as furniture, technology equipment, computer hardware or software, cell phones, electronic services or support, or decorative items. To the extent that items, furniture, technology equipment, computer hardware or software, and/or equipment are needed because of or based on an ADA reasonable accommodation request, please refer to the Agency Reasonable Accommodation Policy for Employees and Applicants with Disabilities.

E. Expenses incurred in connection with normal commuting between home and work, including but not limited to mileage, parking, and toll expenses;

F. Expenses for personal meals or other food or drink items while remaining local and not traveling out of the County on official business;

G. Traffic citations, parking tickets, and other fines, fees, penalties, or costs related to parking or moving violations;

H. Lost or stolen cash or personal property;

I. Monthly payments for leasing personal vehicles, except payments for vehicles leased by an Official for both business and personal use (with reimbursement amount limited to the portion expended for business use) in accordance with Cook County Ordinance Section 34-40 and approved by the Appropriate Authorizing Party;

J. Personal calls;

K. Personal items, including but not limited to toiletries, luggage, clothing, medications, appliances, and decorative items;

L. Personal entertainment items, including but not limited to, magazines, books, movie rentals, and event tickets (sporting, theater, musical, etc), and/or recreational activities;

M. Alcoholic beverages, tobacco products or controlled substances;

N. Food, except as permitted pursuant to Sections III.A. and III.B. below;

O. Supplies for office events;

P. Sponsorships or donations;

Q. Kitchen textiles (e.g. napkins, cups, utensils, etc.);

R. Appliances (e.g. microwaves, refrigerators, toasters);

S. Sporting goods;

T. Flowers, gift cards, and gifts, or similar types of costs;

U. Credit card or other late fees due to the Employee’s or Official’s actions;

V. Charges related to modifications to travel arrangements, including but not limited to itinerary changes or cancellations, unless such change or cancellation is based on an exigent circumstance not within the Employee's or Official's own making and for which the Employee or Official is unable to receive a reimbursement or credit against the travel arrangement;

W. Convenience fees, including but not limited to, early check-in, late check-out, and TSA pre-check;

X. Hotel incidentals, such as, but not limited to, room upgrades, room service, health club fees, in-room entertainment fees, and laundry fees;

Y. Flight insurance or other supplemental travel insurance;

Z. Guest travel costs and expenses;

AA. International travel, without written pre-authorization from the Appropriate Authorizing Party and the Budget Director, as applicable;

BB. Personal portions of a trip combined with business travel, including but not limited to extended stays and travel to/from other destination(s);

CC. Upgrades, including but not limited to, special "club" floors or access, seat or cabin upgrades, premium fuel, premium rides, valet parking; and,

DD. Other expenses of a purely personal nature and not listed as reimbursable in these guidelines.

III. ELIGIBLE REIMBURSABLE NECESSARY BUSINESS EXPENSES

The following expenses are considered Necessary Business Expenses that are eligible for reimbursement contingent on compliance with this policy.

A. <u>Food Supplies</u>

Appropriated Funds shall not be used to purchase food, except in the following limited circumstances.

1. Ceremonial Events: The use of Appropriated Funds to provide light refreshments, such as snacks and beverages, at County sponsored, public facing ceremonial events when it has been determined that such food would materially enhance the event in furtherance of the objectives of the event is permissible.

2. Budget Hearings and Board Meetings: The use of Appropriated Funds by the Secretary to the Board to provide food for Officials and Employees actively participating in budget hearings or board meetings, to facilitate the efficient and timely resolution of such hearings before the Board of Commissioners, is permissible.

3. Community Events: The use of Appropriated Funds to provide light refreshments, such as snacks and beverages, at County sponsored community engagement events when it has been determined that such food would materially enhance public participation in furtherance of the objectives of the event is permissible.

4. Employee Morale Events. The use of Appropriated Funds to provide light refreshments, such as snacks and beverages or to provide lunch, for Officials and/or Employees scheduled to boost Employee morale or in recognition of Employees when it has determined by the hosting Agency that such food would materially enhance participation and boost morale in furtherance of the objectives of the event is permissible. Employee morale events may be hosted occasionally and the cost of any such event is limited to $20 per person.

5. Trainings: The use of Appropriated Funds to provide light refreshments, such as snacks and beverages for training events, or meals at full-day or after hour training events hosted by an Agency is permissible.

B. Registration Fees

Registration fees for non-County government conferences, meetings, seminars, training sessions, professional development, continuing education related to professional licensing requirements or similar events may be reimbursed. Reimbursements may include the cost of any food included in the registration fee. Every effort should be made to take advantage of early registration or group rate discounts. Employees and Officials must execute their registration in accordance with Section IV. below.

C. Professional Licensing Fees and Certifications

Licensing, registration or certification fees that are related to and required by federal, state or local statutes and ordinances that are required as a condition of being hired and holding an employee’s position may be reimbursed. Employees and Officials must execute reimbursements for such requests in accordance with Section IV. below.

D. **Travel Expenses**

In order for an Employee or Official to be eligible for reimbursement for travel expenses, all travel for official County business should be prudently planned so that the County's best interests are served at the most reasonable cost considering travel time and work requirements. Employees and Officials should make best efforts to execute their Local and Non-local travel requirements at the lowest reasonable costs to the County by purchasing ticket(s) in advance, searching for lowest prices, requesting the government rate where available or utilizing a travel agent, etc.

1. Types of Travel that are Eligible for Reimbursement. The County recognizes the following activities as appropriate travel purposes for official County business:

(a) Delivery of legislative testimony or address legislative agenda;

(b) As a stipulation or condition of grant funding or otherwise required for County or federal certification;

(c) Presentation on behalf of the County at a conference, meeting, seminar, training session, or similar;

(d) Financial or tax audit;

(e) Site visit or operational evaluation related to Agency improvement efforts;

(f) Court proceeding or case preparation, where the Employee is appearing on behalf of the County or the Employee needs to engage in witness preparation, investigation or take depositions.

(g) Law enforcement, building and zoning, revenue, ethics, environmental, medical examiner or other investigation approved by the Appropriate Authorizing Party; and

(h) Attendance at a conference, meeting, seminar, training session, or similar, provided that the topic is of critical interest to the County; representation at the event is in the best interest of the County; and the topic is related to an Employee's or Official's professional development. Agencies should attempt to limit the number of attendees by event.

2. <u>Modes of Local Travel</u>. Authorized modes of transportation for Local Travel include: (1) public transportation; (2) County vehicles; (3) taxi, ride sharing; and (4) Personally owned or Leased vehicles (approved by the Appropriate Authorizing Party).

3. <u>Modes of Non-local Travel</u>. Authorized modes of transportation for Non-local travel include County vehicles, Personally owned or Leased vehicles if approved by the Appropriate Authorizing Party, Rental Car, and Common Carriers.

4. <u>General rule for travel</u>. Travel expenses are eligible for reimbursement provided that the least expensive mode of transportation is used, considering travel time, cost, and work requirements unless otherwise approved by the Appropriate Authorizing Party. Please note that employees who receive a stipend are not eligible for mileage reimbursement.

5. <u>Eligible Local Transportation Reimbursable Expenses</u>: Local travel that is performed for official County business may be permissible if authorized by the Appropriate Approving Party.

(a) *Travel by County vehicle*. When the Employee or Official uses a County vehicle, only fuel, parking, and toll expenses are eligible for reimbursement.

(b) *Travel by taxi or ride share*. When the Employee or Official uses a taxi or ride sharing company, the total metered fare (including surcharges and fees) is eligible for reimbursement. Tipping on taxis or ride sharing may not exceed $2.00, or 20% of the metered fare, whichever amount is greater.

(c) *Travel by Personal vehicle*. When the Employee or Official uses a Personal vehicle per the approval of the Appropriate Authorizing Party, only mileage, parking, and toll expenses are eligible for reimbursement. Mileage reimbursement for County business is limited to the current standard IRS deduction rate for business related transportation currently in effect and authorized by the Bureau of Finance. The mileage must be supported by detailed mileage logs including date(s) of travel, number of miles driven, locations traveled to and from, and business purpose. All mileage requested to be reimbursed will be calculated using the County's Transportation Expense Voucher System (TEVS) to prepare a mileage reimbursement voucher which can be found at (https://apps.cookcountyil.gov/voucher/public/). The voucher shall be submitted along with the Business and/or Travel Expense Reimbursement Form to the Appropriate Authorizing Party.

i. Normal commuting to and from the Employee's or Official's Personal residence and their Official Worksite or an Agency pre-approved Alternative Worksite is not eligible for mileage reimbursement. However, if the mileage to an Alternative Worksite is greater than the normal commute to and from the Official Worksite, then the Employee or Official is entitled to reimbursement for mileage in excess of their normal commute.

ii. When approved Local Travel is required during the workday, the Employee or Official is entitled to reimbursement for the mileage to and from the Official Worksite or Alternative Worksite and the site(s) visited. Only the most direct route mileage (mileage from residence to first location and last location to residence is deemed commuting mileage and shall not be reimbursed in the mileage calculator) from the Official Worksite where applicable to the site(s) visited and back to the Official Worksite will be reimbursed.

iii. The IRS per-mile rate is generally established annually (but may be subject to a mid-year increase) and covers the total cost of operating a personally owned vehicle for Local Travel, including such items as gasoline, oil, maintenance, repairs, etc.

iv. The Employee or Official must carry liability and property damage insurance for business use of their Personal or Personally leased vehicle and submit a copy of these insurance policies to the appropriate personnel within their department. The Employee or Official's personal insurance is primary in the event of an accident.

6. Eligible Non-Local Transportation Reimbursable Expenses: Non-Local Travel that is performed for official County business may be permissible if authorized by the Appropriate Approving Party.

(a) *Travel by Personal vehicle*. When the Employee or Official uses a Personal vehicle per the approval of the Appropriate Authorizing Party, only mileage, parking, and toll expenses are eligible for reimbursement. Mileage reimbursement for County business is limited to the current standard IRS deduction rate for business related transportation currently in effect and authorized by the Bureau of Finance. The mileage must be supported by detailed mileage logs including date(s) of travel, number of miles driven, locations traveled to and from, and business purpose. All mileage requested to be reimbursed will be calculated using the mileage calculator in the Transportation Expense Voucher System (TEVS), which shall be submitted along with the Business and/or Travel Expense Reimbursement Form to the Appropriate Authorizing Party.

i. The IRS per-mile rate is generally established annually (but may be subject to a mid-year increase) and covers the total cost of operating a personally owned vehicle for Non-local Travel, including such items as gasoline, oil, maintenance, repairs, etc.

ii. The mileage reimbursement per trip may not exceed the cost of the lowest available non-stop, roundtrip airfare to/from the destination.

iii. The Employee or Official must carry liability and property damage insurance for business use of their Personal or Personally leased vehicle.

(b) *Travel by Rental Car*. Travel by Rental Car is limited to Non-local travel requiring an overnight stay and must be supported by an itemized receipt which lists the date, time, location of the rental, rental rate, and vehicle class. The choice of vehicle class must be reasonable based on the circumstances. When the Employee or Official uses a rental car, only daily rental rates, taxes, surcharges, car rental insurance, fuel, parking, and toll expenses are eligible for reimbursement.

(c) *Travel by Common Carrier*. Travel by common carrier is limited to Non-local travel requiring an overnight stay and must be supported by itemized receipts which list the traveler's name, the date, time, point of origin and destination, fare class purchased, and any other related costs for each leg of the trip. When the Employee or Official uses a common carrier, only the fare, taxes, surcharges, and any standard baggage fees are eligible for reimbursement. The fare reimbursement will be based on the most economical fare available that meets the requirements of the Employee's or Official's agenda.

(d) *International travel*. All international travel is subject to pre-authorization by the Appropriate Authorizing Party and Budget Director. Employee's and Official's shall convert all foreign expenses to U.S. currency at the exchange rate applicable when the expense was paid and reflect the expenses incurred in U.S. dollars on the Business and/or Travel Expense Reimbursement Form. Official documentation of the exchange rate(s) applied to the expenses incurred, published at https://www1.oanda.com/currency/converter/ must accompany all receipts.

(e) *Meal and incidental expense reimbursement*. Meal and incidental expense reimbursements are limited to Non-local travel requiring an overnight stay and must be supported by itemized receipts which list the date, time, location of the purchase, and detail every individual item included on the bill. Examples of reimbursable incidental expenses may include necessary internet connection fees or cellular phone charges related to official business. Employee's and Official's will receive the lesser of the actual costs or the current federal travel allowance for meals and incidental expenses, including taxes and gratuity, which is capped at no more than 20% of cost of meal, published by the General Services Administration at https://www.gsa.gov/travel/plan-book/per-diem-rates. Gratuity for baggage handling is reimbursable so long as the cost is reasonable and does not exceed $5.00 per handling. Reimbursement for meals and incidental expenses shall be limited to the expenses incurred during the time spent traveling for County business. 75% of the expenses submitted for reimbursement on the first and last days of travel, and 100% of the expenses on the other days.

(f) *Lodging reimbursement*. Lodging reimbursement is limited to Non-local travel requiring an overnight stay and must be supported by itemized receipts which list the traveler's name, the date, time, location of the lodging, and detail every individual item included in the bill. Travelers will receive the lesser of the actual costs or the current federal travel allowance for lodging published by the General Services Administration at https://www.gsa.gov/travel/plan-book/per-diem-rates unless the increased rate is approved by the Appropriate Authorizing Party.

(g) *Reimbursement for taxi or ride share*. When the Employee or Official uses a taxi or ride sharing company, the total metered fare (including surcharges and fees) is eligible for reimbursement. Tipping on taxis or ride sharing may not exceed $2.00, or 20% of the ride - whichever amount is greater.

E. **Business needs that cannot be obtained using the methods provided in the Cook County Procurement Code.** On occasion, necessary business needs are unable to be met using the methods provided in the Cook County Procurement Code. The Official or Employee incurring these expenses must demonstrate it is a Necessary Business Expense with a clear and legitimate business purpose. For technology-related necessary business expenses, the Official and Employee incurring the expense must also demonstrate compliance with the Bureau of Technology's Concurrence Process or other similarly applicable policy.

F. **Miscellaneous**. Any other Necessary Business Expense or loss incurred within the Official's or Employee's scope of employment or related to telecommuting and directly related to services performed for the employer as permitted under Illinois Wage Payment and Collection Act, 820 ILCS 115 et. seq.

IV. PROCESS FOR REQUESTING PRE-AUTHORIZATION FOR ELIGIBLE NECESSARY BUSINESS EXPENSES AND SEEKING REIMBURSEMENT

A. **General:** Being reimbursed for a Necessary Business Expense reimbursement is contingent on compliance with the provisions of this policy; obtaining the appropriate pre-authorization; and completion and timely submission of the appropriate forms with supporting documentation, including but not limited to original receipts. Receipts must be legible; electronic copies including clear photographs of receipts will be accepted as originals. Where supporting documentation does not exist or is missing or lost, the Employee or Official shall submit the Affidavit for Lost Receipts form regarding any such receipts.

B. **Pre-Authorization to Incur a Necessary Business Expense:** Employees and Officials are required to obtain pre-approval before incurring any Necessary Business Expense by submitting the Pre-Authorization Form to the Appropriate Authorizing Party, and in the case of international travel, the Pre-Authorization Form must also be submitted to the Budget Director. Employees and Officials shall request authorization to incur a Necessary Business Expense using the Pre-Authorization Form at least thirty (30) calendar days in advance of having to incur the expenditure or loss so the Appropriate Authorizing Party has an opportunity to assess and potentially approve the request in accordance with this policy. If the pre-authorization or the thirty (30) day period is not practicable, the Requester must provide a justification on the Pre-Authorization Form and/or Reimbursement Form for deviating from the 30 day requirement.

1. Eligible Necessary Business Expenses other than travel.

The Pre-Authorization Form must be completed by the Requester and sent to the Appropriate Approving Party supported by:

i. the details of the expense(s) to be incurred, including the amount and when and where the purchase or expense will be made;

ii. the reason and purpose of the purchase or expense; and

iii. why the item is not being purchased using the methods provided in the Cook County Procurement Code.

2. Travel Expenses.

(a) To request Local or Non-local travel authorization, the Pre-Authorization Form must be completed by the Requester and sent to the Appropriate Approving Party supported by an agenda and estimate of travel costs. The Documentation regarding anticipated meal and lodging costs shall be included along with the current federal travel allowance for lodging and per diem meal rates published by the General Services Administration at https://www.gsa.gov/travel/plan-book/per-diem-rates.

(b) For regularly re-occurring Local or Non-local travel that would be considered a Necessary Business Expense, the Appropriate Approving Party has the discretion to establish a process to pre-approve such travel.

C. **Appropriate Authorizing Party.** To authorize incurring Necessary Business Expenses, the Pre-Authorization Form must be reviewed and approved by the Appropriate Authorizing Party. By signing the Pre-Authorization Form, the Appropriate Authorizing Party certifies:

1. the expenditure is a Necessary Business Expense as provided by this policy, including the appropriateness of the expenditure and the reasonableness of the amount;

2. the Requester has submitted a completed and accurate Pre-Authorization Form with required supporting documentation; and

3. Appropriate Funding is available to pay for the expense.

In addition, if the Appropriate Authorizing Party determines that the requested expenditure is not necessary or should be requested through the Procurement Code process, then the Employee or Official shall not incur the expense on the County's behalf and will not be entitled to reimbursement under this policy.

D. **Submission of Reimbursement Requests, Review and Approval.**

1. All requests seeking reimbursement, with the appropriate supporting documentation and Business and/or Travel Expense Reimbursement Form, must be submitted to the Appropriate Authorizing Party within 60 calendar days of the later of (1) incurring the expense or (2) the business purpose, travel, or event has occurred. By signing the Business and/or Travel Expense Reimbursement Form, the Requester attests to its truthfulness and assumes personal responsibility for its accuracy.

2. Submission of the Business and/or Travel Expense Reimbursement Form to the Appropriate Authorizing Party shall also include:

(a) A copy of the approved Pre-Authorization Form;

(b) Copies of itemized receipts for all expenses; and

(c) If a receipt is lost or does not exist, the Requester needs to complete the Affidavit for Lost Receipts Form to attest to the incurring of such expense and why no documentation is being submitted to support the particular expense reimbursement request.

3. Within 21 calendar days of receipt of the Business and/or Travel Expense Reimbursement request, the approved request by the Appropriate Authorizing Party and the supporting documentation shall be sent by the Appropriate Authorizing Party to the department's assigned Budget Analyst in Budget. By approving the reimbursement request and forwarding to the Budget Analyst, the Appropriate Authorizing Party certifies the appropriateness of the expenditure and the reasonableness of the amount; the availability of Appropriated Funds; compliance with applicable reimbursement policies; and completeness of supporting documentation.

4. Review of all requests for reimbursement shall be timely made by Budget. Upon review, Budget will approve the request, return the request to the Appropriate Approving Party for correction or supplementation (i.e., credit card statement and Affidavit for Lost Receipts Form, in the event of lost receipts), or deny the request as not being in compliance with this Policy. If approved, Budget will submit the reimbursement request to the Comptroller's Office for payment and copy the Appropriate Authorizing Party regarding the payment request. Failure to timely correct or supplement a request for reimbursement as required by Budget shall result in denial of reimbursement.

5. <u>Timing and method of reimbursement payment</u>. Employees or Officials will receive authorized reimbursements as part of their next regular paycheck during the pay period following the expense having been incurred, and the reimbursement request being processed, provided compliance with this Policy and the procedures established herein. Advanced payments to the requestor are strictly prohibited under this policy.

E. Resources

General information concerning this Policy may be obtained by contacting the Chief Financial Officer (or designee).

F. Related Policies

- The Cook County Procurement Code
- The County's Vehicle Collision Policy
- The County's Fuel Use Policy
- The County's AVL GPS Policy
- The County's Vehicle Policy
- Applicable Agency Reasonable Accommodation Policy for Employees and Applicants with Disabilities
- Applicable Agency Telecommuting Policy
- Applicable Agency Tuition Reimbursement Policy
- The County's Ethics Ordinance

G. Non-Compliance

Failure to comply with the provisions of this policy may result in denial of reimbursement and/or subject an Employee or Official to discipline, up to and including discharge, in accordance with the personnel rules and/or collective bargaining agreement, if applicable, and ethics fines or penalties.

EXHIBIT 11

Economic Disclosure Statement

COOK COUNTY ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT INDEX

SECTION 1
INSTRUCTIONS FOR COMPLETION OF
ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every Proposer responding to a Request for Proposals, and every Respondent responding to a Request for Qualifications, and others as required by the Chief Procurement Officer. The execution of the EDS shall serve as the execution of a contract awarded by the County. The Chief Procurement Officer reserves the right to request that the Bidder or Proposer, or Respondent provide an updated EDS on an annual basis.

Definitions. Terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, as applicable.

Affiliate means a person that directly or indirectly through one or more intermediaries, Controls is Controlled by, or is under common Control with the Person specified.

Applicant means a person who executes this EDS.

Bidder means any person who submits a Bid.

Code means the Code of Ordinances, Cook County, Illinois available on municode.com.

Contract shall include any written document to make Procurements by or on behalf of Cook County.

Contractor or *Contracting Party* means a person that enters into a Contract with the County.

Control means the unfettered authority to directly or indirectly manage governance, administration, work, and all other aspects of a business.

EDS means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.

Joint Venture means an association of two or more Persons proposing to perform a for-profit business enterprise. Joint Ventures must have an agreement in writing specifying the terms and conditions of the relationship between the partners and their relationship and respective responsibility for the Contract

Lobby or lobbying means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.

Lobbyist means any person who lobbies.

Person or *Persons* means any individual, corporation, partnership, Joint Venture, trust, association, Limited Liability Company, sole proprietorship or other legal entity.

Prohibited Acts means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

Proposal means a response to an RFP.

Proposer means a person submitting a Proposal.

Response means response to an RFQ.

Respondent means a person responding to an RFQ.

RFP means a Request for Proposals issued pursuant to this Procurement Code.

RFQ means a Request for Qualifications issued to obtain the qualifications of interested parties.

INSTRUCTIONS FOR COMPLETION OF ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

Section 1: Instructions. Section 1 sets forth the instructions for completing and executing this EDS.

Section 2: Certifications. Section 2 sets forth certifications that are required for contracting parties under the Code and other applicable laws. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

Section 3: Economic and Other Disclosures Statement. Section 3 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Applicant to the warranties, representations, agreements and acknowledgements contained therein.

Required Updates. The Applicant is required to keep all information provided in this EDS current and accurate. In the event of any change in the information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Applicant shall supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is required.

Additional Information. The County's Governmental Ethics and Campaign Financing Ordinances impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions, and the Applicant is expected to comply fully with these ordinances. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit the web-site at cookcountyil.gov/ethics-board-of.

Authorized Signers of Contract and EDS Execution Page. If the Applicant is a corporation, the President and Secretary must execute the EDS. In the event that this EDS is executed by someone other than the President, attach hereto a certified copy of that section of the Corporate By-Laws or other authorization by the Corporation, satisfactory to the County that permits the person to execute EDS for said corporation. If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a partnership or joint venture, all partners or joint venturers must execute the EDS, unless one partner or joint venture has been authorized to sign for the partnership or joint venture, in which case, the partnership agreement, resolution or evidence of such authority satisfactory to the Office of the Chief Procurement Officer must be submitted with this Signature Page.

If the Applicant is a member-managed LLC all members must execute the EDS, unless otherwise provided in the operating agreement, resolution or other corporate documents. If the Applicant is a manager-managed LLC, the manager(s) must execute the EDS. The Applicant must attach either a certified copy of the operating agreement, resolution or other authorization, satisfactory to the County, demonstrating such person has the authority to execute the EDS on behalf of the LLC. If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a Sole Proprietorship, the sole proprietor must execute the EDS.

A "Partnership" "Joint Venture" or "Sole Proprietorship" operating under an Assumed Name must be registered with the Illinois county in which it is located, as provided in 805 ILCS 405 (2012), and documentation evidencing registration must be submitted with the EDS.

Effective October 1, 2016 all foreign corporations and LLCs must be registered with the Illinois Secretary of State's Office unless a statutory exemption applies to the applicant. Applicants who are exempt from registering must provide a written statement explaining why they are exempt from registering as a foreign entity with the Illinois Secretary of State's Office.

CONTRACT #: #2112-18598

SECTION 2

CERTIFICATIONS

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE APPLICANT IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE APPLICANT THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE APPLICANT IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE APPLICANT SHALL BE SUBJECT TO TERMINATION.

A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;

2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.;*

3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;

4) Has been convicted of an act committed, within the State**,** of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.;*

5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;

6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;

7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or

8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in sub-paragraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20% or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

***THE APPLICANT HEREBY CERTIFIES THAT*:** The Applicant has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Applicant has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Applicant would not violate the provisions of such Section or of the Code.

B. BID-RIGGING OR BID ROTATING

THE APPLICANT HEREBY CERTIFIES THAT: *In accordance with 720 ILCS 5/33 E-11, neither the Applicant nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.*

C. DRUG FREE WORKPLACE ACT

***THE APPLICANT HEREBY CERTIFIES THAT*:** The Applicant will provide a drug free workplace, as required by (30 ILCS 580/3).

D. DELINQUENCY IN PAYMENT OF TAXES

THE APPLICANT HEREBY CERTIFIES THAT*: The Applicant is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-171.*

E. HUMAN RIGHTS ORDINANCE

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 *et seq.*).

F. ILLINOIS HUMAN RIGHTS ACT

THE APPLICANT HEREBY CERTIFIES THAT: *It is in compliance with the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

G. INSPECTOR GENERAL (COOK COUNTY CODE, CHAPTER 34, SECTION 34-174 and Section 34-250)

The Applicant has not willfully failed to cooperate in an investigation by the Cook County Independent Inspector General or to report to the Independent Inspector General any and all information concerning conduct which they know to involve corruption, or other criminal activity, by another county employee or official, which concerns his or her office of employment or County related transaction.

The Applicant has reported directly and without any undue delay any suspected or known fraudulent activity in the County's Procurement process to the Office of the Cook County Inspector General.

H. CAMPAIGN CONTRIBUTIONS (COOK COUNTY CODE, CHAPTER 2, SECTION 2-585)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning campaign contributions, which is codified at Chapter 2, Division 2, Subdivision II, Section 585, and can be read in its entirety at www.municode.com.

I. GIFT BAN, (COOK COUNTY CODE, CHAPTER 2, SECTION 2-574)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning receiving and soliciting gifts and favors, which is codified at Chapter 2, Division 2, Subdivision II, Section 574, and can be read in its entirety at www.municode.com.

J. LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-160;

Unless expressly waived by the Cook County Board of Commissioners, the Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is annually by the Chief Financial Officer of the County, and shall be posted on the Chief Procurement Officer's website.

The term "Contract" as used in Section 4, I, of this EDS, specifically excludes contracts with the following:

1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United State Internal Revenue Code and recognized under the Illinois State not-for -profit law);

2) Community Development Block Grants;

3) Cook County Works Department;

4) Sheriff's Work Alternative Program; and

5) Department of Correction inmates.

SECTION 3

REQUIRED DISCLOSURES

1. DISCLOSURE OF LOBBYIST CONTACTS

List all persons that have made lobbying contacts on your behalf with respect to this contract:

Name Address

NA

2. LOCAL BUSINESS PREFERENCE STATEMENT (CODE, CHAPTER 34, SECTION 34-230)

Local business means a Person, including a foreign corporation authorized to transact business in Illinois, having a bona fide establishment located within the County at which it is transacting business on the date when a Bid is submitted to the County, and which employs the majority of its regular, full-time work force within the County. A Joint Venture shall constitute a Local Business if one or more Persons that qualify as a "Local Business" hold interests totaling over 50 percent in the Joint Venture, even if the Joint Venture does not, at the time of the Bid submittal, have such a bona fide establishment within the County.

a) Is Applicant a "Local Business" as defined above?

Yes: □ No: ☑

b) If yes, list business addresses within Cook County:

c) Does Applicant employ the majority of its regular full-time workforce within Cook County?

Yes: □ No: ☑

3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (CODE, CHAPTER 34, SECTION 34-172)

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-5) and complete the Affidavit, based on the instructions in the Affidavit.

4. REAL ESTATE OWNERSHIP DISCLOSURES.

The Applicant must indicate by checking the appropriate provision below and providing all required information that either:

a) The following is a complete list of all real estate owned by the Applicant in Cook County:

PERMANENT INDEX NUMBER(S): ______________________________

____

____

(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX NUMBERS)

OR:

b) ☑ The Applicant owns no real estate in Cook County.

5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.

If the Applicant is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Applicant must explain below:

If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Applicant certified to all Certifications and other statements contained in this EDS.

CONTRACT #:#2112-18598

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"*Applicant*" means any Entity or person making an application to the County for any County Action.

"County Action" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"Person" "Entity" or *"Legal Entity"* means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and

2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the [☑] Applicant or [□] Stock/Beneficial Interest Holder

This Statement is an: [☑] Original Statement or [□] Amended Statement

Identifying Information:

Name KAPSTONE TECHNOLOGIES LLC

D/B/A: KAPSTONE LLC FEIN # Only: 46 4164595

Street Address: 370 CAMPUS DRIVE #108

City: SOMERSET State: NJ Zip Code: 08873

Phone No.: 7324253980 Fax Number: Email: HARISH.JANGADA@

Cook County Business Registration Number:
(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable): 05995418

Form of Legal Entity:

□ Sole Proprietor ☑ Partnership □ Corporation □ Trustee of Land Trust

□ Business Trust □ Estate □ Association □ Joint Venture

□ Other (describe)

Ownership Interest Declaration:

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
iC Consult GMBH	80 Pine Street, Floor 24, New York,NY, 1005	100%

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
N/A		

3. Is the Applicant constructively controlled by another person or Legal Entity? [☑] Yes [□] No

If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship
iC Consult GMBH	80 Pine Street, Floor 24, New York,NY, 1005	100%.	Parent co.

Corporate Officers, Members and Partners Information:

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
Harish Jangada	370 Campus Drive#108, somerset,NJ-08873.	Partner.	Since Apr 2016
Pravin Patil	370 Campus Drive#108, somerset,NJ-08873.	Partner.	Since Apr 2016
Saurabh Sharma	370 Campus Drive#108, somerset,NJ-08873.	Partner.	Since Apr 2016

Declaration (check the applicable box):

☑ I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.

☑ I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

Harish Jangada	Partner
Name of Authorized Applicant/Holder Representative (please print or type)	Title
Jangada	
Signature	Date
harish.jangada@kapstonellc.com	7324253980
E-mail address	Phone Number

Subscribed to and sworn before me
this 3rd day of Oct , 2022

My commission expires: 07/24/2025

x
Notary Public Signature

Notary Seal

NASER R. BATAH
NOTARY PUBLIC, STATE OF NEW JERSEY
COMMISSION # 50132485
MY COMMISSION EXPIRES
JULY 24, 2025

CONTRACT #:#2112-18598

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing. **County reserves the right to request additional information to verify veracity of information contained in this statement.**

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"*Applicant*" means any Entity or person making an application to the County for any County Action.

"County Action" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"Person" "Entity" or *"Legal Entity"* means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and

2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the [☑] Applicant or [☐] Stock/Beneficial Interest Holder

This Statement is an: [☑] Original Statement or [☐] Amended Statement

Identifying Information:

Name iC Consult GMBH

D/B/A: iC Consult Corp FEIN # Only: 46-3751618

Street Address: 80 Pine Street Floor 24

City: New York State: NY Zip Code: 10005

Phone No.: 7324253980 Fax Number: Email: harish.jangada@ic-co

Cook County Business Registration Number:
(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable):

Form of Legal Entity:

☐ Sole Proprietor ☐ Partnership ☑ Corporation ☐ Trustee of Land Trust

☐ Business Trust ☐ Estate ☐ Association ☐ Joint Venture

☐ Other (describe)

CONTRACT #:#2112-18598

Ownership Interest Declaration:

1. List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
N/A		

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
N/A		

3. Is the Applicant constructively controlled by another person or Legal Entity? [□] Yes [□] No

If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship
N/A			

Corporate Officers, Members and Partners Information:

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
Jonathan Edwards.	80 pine st, New york, NY	CEO Americas.	Since Jan 2022
Volker Witzel	80 Pine St, New York, Ny.	Group CEO	Since Aug. 2022

Declaration (check the applicable box):

☑ I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.

☑ I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

CONTRACT #:#2112-18598

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

Harish Jangada
Name of Authorized Applicant/Holder Representative (please print or type)

EVP, Chief Product Officer
Title

Signature

01/05/2024
Date

harish.jangada@kapstonellc.com
E-mail address

7324253980
Phone Number

Subscribed to and sworn before me
this 5 day of 01, 2024

X Vinay Kumar
Notary Public Signature

My commission expires: 7/28/26

Notary Seal

VINAY KUMAR
Notary Public, State of New Jersey
My Commission Expires Jul 28, 2026

COOK COUNTY BOARD OF ETHICS
69 W. WASHINGTON STREET, SUITE 3040
CHICAGO, ILLINOIS 60602
312/603-4304 Office 312/603-9988 Fax

FAMILIAL RELATIONSHIP DISCLOSURE PROVISION

Nepotism Disclosure Requirement:

Doing a significant amount of business with the County requires that you disclose to the Board of Ethics the existence of any familial relationships with any County employee or any person holding elective office in the State of Illinois, the County, or in any municipality within the County. The Ethics Ordinance defines a significant amount of business for the purpose of this disclosure requirement as more than $25,000 in aggregate County leases, contracts, purchases or sales in any calendar year.

If you are unsure of whether the business you do with the County or a County agency will cross this threshold, err on the side of caution by completing the attached familial disclosure form because, among other potential penalties, any person found guilty of failing to make a required disclosure or knowingly filing a false, misleading, or incomplete disclosure will be prohibited from doing any business with the County for a period of three years. The required disclosure should be filed with the Board of Ethics by January 1 of each calendar year in which you are doing business with the County and again with each bid/proposal/quotation to do business with Cook County. The Board of Ethics may assess a late filing fee of $100 per day after an initial 30-day grace period.

The person that is doing business with the County must disclose his or her familial relationships. If the person on the County lease or contract or purchasing from or selling to the County is a business entity, then the business entity must disclose the familial relationships of the individuals who are and, during the year prior to doing business with the County, were:

- its board of directors,
- its officers,
- its employees or independent contractors responsible for the general administration of the entity,
- its agents authorized to execute documents on behalf of the entity, and
- its employees who directly engage or engaged in doing work with the County on behalf of the entity.

Do not hesitate to contact the Board of Ethics at (312) 603-4304 for assistance in determining the scope of any required familial relationship disclosure.

Additional Definitions:

"*Familial relationship*" means a person who is a spouse, domestic partner or civil union partner of a County employee or State, County or municipal official, or any person who is related to such an employee or official, whether by blood, marriage or adoption, as a:

□ Parent
□ Child
□ Brother
□ Sister
□ Aunt
□ Uncle
□ Niece
□ Nephew

□ Grandparent
□ Grandchild
□ Father-in-law
□ Mother-in-law
□ Son-in-law
□ Daughter-in-law
□ Brother-in-law
□ Sister-in-law

□ Stepfather
□ Stepmother
□ Stepson
□ Stepdaughter
□ Stepbrother
□ Stepsister
□ Half-brother
□ Half-sister

CONTRACT #:#2112-18598

COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM

A. PERSON DOING OR SEEKING TO DO BUSINESS WITH THE COUNTY

Name of Person Doing Business with the County: Kapstone Technologies LLC

Address of Person Doing Business with the County: 370 Campus Drive # 108, Somerset, NJ - 08873

Phone number of Person Doing Business with the County: 732 356 5130

Email address of Person Doing Business with the County: harish.jangada@kapstonellc.com

If Person Doing Business with the County is a Business Entity, provide the name, title and contact information for the individual completing this disclosure on behalf of the Person Doing Business with the County:

Harish Jangada, Managing Partner - harish.jangada@kapstonellc.com

B. DESCRIPTION OF BUSINESS WITH THE COUNTY

Append additional pages as needed and for each County lease, contract, purchase or sale sought and/or obtained during the calendar year of this disclosure (or the proceeding calendar year if disclosure is made on January 1), identify:

The lease number, contract number, purchase order number, request for proposal number and/or request for qualification number associated with the business you are doing or seeking to do with the County: #2112-18598

The aggregate dollar value of the business you are doing or seeking to do with the County: $9,680,967.00

The name, title and contact information for the County official(s) or employee(s) involved in negotiating the business you are doing or seeking to do with the County: Yaneth Lopez, Procurement Manager

yaneth.lopez@cookcountyil.gov

The name, title and contact information for the County official(s) or employee(s) involved in managing the business you are doing or seeking to do with the County: Hema Sundaram, Chief Technology Officer,

Hema.Sundaram@cookcountyil.gov

C. DISCLOSURE OF FAMILIAL RELATIONSHIPS WITH COUNTY EMPLOYEES OR STATE, COUNTY OR MUNICIPAL ELECTED OFFICIALS

Check the box that applies and provide related information where needed

□ The Person Doing Business with the County **is an individual** and there is **no familial relationship** between this individual and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

☒ The Person Doing Business with the County **is a business entity** and there is **no familial relationship** between any member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity or employees directly engaged in contractual work with the County on behalf of the business entity, and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

CONTRACT #:#2112-18598

COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM

□ The Person Doing Business with the County **is an individual** and **there is a familial relationship** between this individual and at least one Cook County employee and/or a person or persons holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County. **The familial relationships are as follows:**

Name of Individual Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

If more space is needed, attach an additional sheet following the above format.

□ The Person Doing Business with the County **is a business entity** and **there is a familial relationship** between at least one member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity and/or employees directly engaged in contractual work with the County on behalf of the business entity, on the one hand, and at least one Cook County employee and/or a person holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County, on the other. **The familial relationships are as follows**:

Name of Member of Board of Director for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

Name of Officer for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

Name of Person Responsible for the General Administration of the Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

Name of Agent Authorized to Execute Documents for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

Name of Employee of Business Entity Directly Engaged in Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
N/A			

If more space is needed, attach an additional sheet following the above format.

VERIFICATION: To the best of my knowledge, the information I have provided on this disclosure form is accurate and complete. I acknowledge that an inaccurate or incomplete disclosure is punishable by law, including but not limited to fines and debarment.

Signature of Recipient

01/03/2024
Date

SUBMIT COMPLETED FORM TO: Cook County Board of Ethics
69 West Washington Street, Suite 3040, Chicago, Illinois 60602
Office (312) 603-4304 – Fax (312) 603-9988
CookCounty.Ethics@cookcountyil.gov

* Spouse, domestic partner, civil union partner or parent, child, sibling, aunt, uncle, niece, nephew, grandparent or grandchild by blood, marriage (*i.e.* in laws and step relations) or adoption.

SECTION 4

COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE

Effective May 1, 2015, every Person, ***including Substantial Owners***, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"*Contract*" means any written document to make Procurements by or on behalf of Cook County.

"*Person*" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"*Procurement*" means obtaining supplies, equipment, goods, or services of any kind.

"*Substantial Owner*" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information. **County reserves the right to request additional information to verify veracity of information contained in this Affidavit.**

I. Contract Information:

Contract Number: #2112-18598

County Using Agency (requesting Procurement): Bureau of Technology.

II. Person/Substantial Owner Information:

Person (Corporate Entity Name): Kapstone Technologies LLC

Substantial Owner Complete Name: iC Consult GMBH

FEIN# 46-4163595

[redacted] E-mail address: harish.jangada@kapstonellc.cor

Street Address: 370 campus drive #108

City: somerset State: nj Zip: 08873

Home Phone: [redacted]

III. Compliance with Wage Laws:

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

No	*Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq.,* ***YES or NO***
No	*Illinois Minimum Wage Act, 820 ILCS 105/1 et seq.,* ***YES or NO***
No	*Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq.,* ***YES or NO***
No	*Employee Classification Act, 820 ILCS 185/1 et seq.,* **YES or NO**
No	*Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq.,* ***YES or NO***
No	*Any comparable state statute or regulation of any state, which governs the payment of wages* ***YES or NO***

If the Person/Substantial Owner answered **"Yes"** to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV.**

IV. Request for Waiver or Reduction

If Person/Substantial Owner answered **"Yes"** to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction of waiver is made on the basis of one or more of the following actions that have taken place:

No There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner. YES or NO

No Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation. YES or NO

No Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default. YES or NO

No Other factors that the Person or Substantial Owner believe are relevant. YES or NO

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

V. Affirmation

The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

Signature: ______________________ Date: 10/03/22

Name of Person signing (Print): Harish Jangada Title: Managing Partner

Subscribed and sworn to before me this 3rd day of oct., 2022

X______________________ ______________________

Notary Public Signature **Notary Seal**

Note: The above information is subject to verification prior to the award of the Contract.

NASER R . BATAH
NOTARY PUBLIC, STATE OF NEW JERSEY
COMMISSION # 50132485
MY COMMISSION EXPIRES
JULY 24 , 2025

NASER R. BATAH NOTARY PUBLIC NEW JERSEY

SECTION 5

CONTRACT AND EDS EXECUTION PAGE

The Applicant hereby certifies and warrants that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Applicant is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Applicant with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Applicant in this EDS are true, complete and correct. The Applicant agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

Execution by Corporation

Corporation's Name: ____________________

President's Printed Name and Signature: ____________________

Telephone: ____________________

Email: ____________________

Secretary Signature: ____________________

Date: ____________________

Execution by LLC

Kapstone Technologies LLC
LLC Name

Harish Jangada Jangada
*Member/Manager Printed Name and Signature

09/16/2022
Date

7323565130. harish.jangada@kapstonellc.com
Telephone and Email

Execution by Partnership/Joint Venture

Partnership/Joint Venture Name: ____________________

*Partner/Joint Venturer Printed Name and Signature: ____________________

Date: ____________________

Telephone and Email: ____________________

Execution by Sole Proprietorship

Printed Name Signature: ____________________

Assumed Name (if applicable): ____________________

Date: ____________________

Telephone and Email: ____________________

Subscribed and sworn to before me this
3rd day of Oct, 2022

Notary Public Signature

My commission expires: 07/24/2025

NASER R . BATAH
NOTARY PUBLIC, STATE OF NEW JERSEY
COMMISSION # 50132485
MY COMMISSION EXPIRES
JULY 24 , 2025

Notary Seal

*If the operating agreement, partnership agreement or governing documents requiring execution by multiple members, managers, partners, or joint venturers, please complete and execute additional Contract and EDS Execution Pages.

COOK COUNTY SIGNATURE PAGE

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS HEREBY EXECUTED BY:

Raffi Sarrafian Digitally signed by Raffi Sarrafian
Date: 2024.03.15 15:25:03 -05'00'

COOK COUNTY CHIEF PROCUREMENT OFFICER

DATED AT CHICAGO, ILLINOIS THIS_______DAY OF______________________________, 20________

APPROVED AS TO FORM:

Brian Tracy

ASSISTANT STATES ATTORNEY
(Required on contracts over $1,000,000)

CONTRACT TERM & AMOUNT

2112-18598
CONTRACT #

March 04, 2024 through March 03, 2029 **with two (2), one-year renewal options**
ORIGINAL CONTRACT TERM RENEWAL OPTIONS (If Applicable)

$9,680,967.00
CONTRACT AMOUNT

February 29, 2024
COOK COUNTY BOARD APPROVAL DATE (If Applicable)

APPROVED BY THE BOARD OF
COOK COUNTY COMMISSIONERS
FEB 29 2024
COM ______________________