California Health and Human Services Agency
Office of Technology and Solutions Integration
2870 Gateway Oaks Drive, Suite 150
Sacramento, California 95833

REQUEST FOR QUOTE
CalHHS OTSI RFQ #: 75350775

Child Welfare Digital Services
Keeper Renewal

The California Health and Human Services Agency, Office of Technology and Solutions Integration (hereinafter referred to as "CalHHS OTSI" or "State") is inviting you to review and respond to this solicitation for Keeper Renewal. The items are listed in Section 1. Quote Items.

This solicitation is being conducted under the authority of the California Public Contract Code (PCC) Section 12100, purchasing authority for information technology (IT) goods and services.

The CalHHS OTSI has selected to use the Small Business (SB) Option (GC Section 14838.5). To be considered for this solicitation, the vendor must hold a current SB certification.

Responses must comply with the instructions and requirements found herein. Failure to comply with any of the instructions or requirements may cause the response to be rejected. Award will be made to the bidder deemed responsive by meeting all the stated requirements. The State may modify any part of the solicitation by issuance of one (1) or more addenda.

ACSD CONTACT AND KEY ACTION DATES

All Vendors must submit the response electronically via e-mail to the Acquisition and Contracting Services Division (ACSD) Procurement Analyst by the Response Due Date identified below.

ACSD CONTACT	
Procurement Analyst:	Juan Pimentel
Phone Number:	(916) 263-3264
E-mail Address:	Juan.pimentel@otsi.ca.gov
KEY ACTION DATES	
Solicitation Release Date:	July 22, 2026
Response Due Date:	July 28, 2026

1. QUOTE ITEMS

Please provide the Quote to the following items.

Item	Qty	Part Number	Description
1.	75	KS-GOV-PAM	FedRAMP Keeper Privileged Access Manager - Add-On Includes advanced Privileged Access Management (PAM) functionality, along with Keeper Connection Manager, Keeper Secrets Manager, and Remote Browser Isolation. Requires a Keeper Business or Enterprise Password Manager license.
2.	1	KS-GOVSTORAGE_100_GB	Keeper - FedRAMP 100 GB Storage GOV ONLY: Keeper - 100 GB Storage.
3.	500	KS-GOV-AUDIT	Keeper - FedRAMP Advanced Reporting & Alerts Module GOV ONLY: Prevent, detect and isolate security threats.
4.	500	KS-GOVBREACHWATCH	Keeper - FedRAMP BreachWatch for Business GOV ONLY: BreachWatch for Business
5.	500	KS-GOV-COMPLIANCE	Keeper - FedRAMP Compliance Reporting Gov Cloud ONLY Keeper - Compliance Reporting
6.	500	KEEPER-GOVSECURITY-ENT	Keeper - Enterprise Base Plan User Licenses GOV ONLY: Term-based subscription for access to Keeper on unlimited devices.
7.	1	KS-GOV-Platinum-Support	Support Platinum Plan- FEDRAMP Support Platinum Plan Includes the following:> Unlimited Email> Unlimited Automated Chat> Unlimited Live Chat> Unlimited Phone Calls

2. TERM

The term is from August 9, 2026 through August 8, 2027.

3. SUBMITTAL INSTRUCTIONS

The following requirements must be met. Failure to comply with any of the requirements may cause the response to be rejected.

A. Vendor must submit the response via e-mail to the Procurement Analyst by the due date provided in the Key Action Dates. The subject line shall include the CalHHS OTSI RFQ number and the procurement title.

B. The response must be submitted on company's letterhead and include company name, sales representative name, address, phone number, and email address.

C. The response must contain the following:

1) Price for the item(s)
2) Sales tax (if applicable)
3) Discounts offered
4) Total cost

5) Number of days or date the Quote is valid (must be valid for a minimum of 30 days)

4. BIDDER INSTRUCTIONS

Bidder Instructions (GSPD-451) are incorporated by reference and can be accessed here: https://www.dgs.ca.gov/-/media/Divisions/PD/PTCS/GSPD/Bidders-Instructions.pdf. Vendors are advised to review the Bidder Instructions in addition to this solicitation to ensure submission of a responsive bid.

5. AWARD DETERMINATION

Award of an Agreement will be based on best value and meeting all the solicitation requirements.

6. SUBMITTAL REQUIREMENTS

The following documents shall be submitted with the response. If you are unable to access the links below, please refer to: www.osi.ca.gov/Doing_Business_with_OSI.html.

A. Bidder Declaration (GSPD-05-105)

B. Commercially Useful Function (CUF) Documentation (Required if Vendor or subcontractor is a SB/DVBE)

C. DVBE Declarations (DGS PD 843) (Required if Vendor or subcontractor is a DVBE)

D. Federal Debarment, Suspension, Ineligibility and Voluntary Exclusion Certification

E. Civil Rights Certification (Required if amount equals or exceeds $100,000)

F. Iran Contracting Act Certification (Required if amount equals or exceeds $1,000,000)

G. Payee Data Record (STD 204) (Required if Vendor has not previously provided the STD. 204 to the State or if Vendor needs to update information)

H. GenAI Written Notification per Section 7 (If applicable)

I. Seller's Permit (Required for any tangible personal property purchase)

J. Postconsumer Recycled-Content Certification (CalRecycle 74) (Required for any tangible products that fall within the 16 specified product categories)

7. MANDATORY GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

The State of California seeks to realize the potential benefits of GenAI, through the development and deployment of GenAI, while balancing the risks of these technologies.

Bidder/Offeror must notify the State in writing if it: (1) intends to provide GenAI as a deliverable to the State; or (2), intends to utilize GenAI, including GenAI from third parties, to complete all or a portion of any deliverable that materially impacts: (i) functionality of a State system, (ii) risk to the State, or (iii) Contract performance. For avoidance of doubt, the term "materially impacts" shall have the meaning set forth in State Administrative Manual (SAM) 4986.2.

Failure to report GenAI to the State may result in disqualification. The State reserves its right to seek any and all relief it may be entitled to as a result of such non-disclosure.

Upon notification by a Bidder/Offeror of GenAI as required, the state reserves the right to incorporate GenAI Special Provisions into the final contract or reject bids/offers that present an unacceptable level of risk to the state.

Government Code 11549.64 defines "Generative Artificial Intelligence (GenAI)" as an artificial intelligence system that can generate derived synthetic content, including text, images, video, and audio that emulates the structure and characteristics of the system's training data.

8. EXECUTIVE ORDER N-6-22 – RUSSIA SANCTIONS

On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. "Economic Sanctions" refers to sanctions imposed by the U.S. government in response to Russia's actions in Ukraine, as well as any sanctions imposed under state law. By submitting a bid or proposal, Contractor represents that it is not a target of Economic Sanctions. Should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that shall be grounds for rejection of the Contractor's bid/proposal any time prior to contract execution, or, if determined after contract execution, shall be grounds for termination by the State.

9. PROHIBITION ON TAX DELINQUENTS

Public Contract Code (PCC) section 10295.4 prohibits vendors identified as the largest tax delinquents by the Franchise Tax Board (FTB) or the California Department of Tax and Fee Administration (CDTFA) from entering into any contract with the State. Any vendor identified by FTB or CDTFA as a tax delinquent under this section shall be deemed non-responsive and their offer will be rejected.

10. GENERAL PROVISIONS

The Agreement awarded as a result of this solicitation shall incorporate the following terms and conditions. The State will not accept Vendor Quote if additional terms and conditions are included.

IT General Provisions – Cloud Computing Services (Revised and Effective 02/20/2025) published at: https://www.dgs.ca.gov/%7E/media/Divisions/PD/Acquisitions/Solicitation-Document-Attachments/IT-General-Provisions-Cloud-DGS-PD-402ITGP-Revised-02202025.pdf

EXHIBIT A
STATEMENT OF WORK
Child Welfare Digital Services
Keeper Renewal

1. PURPOSE – GENERAL

This Statement of Work (SOW) sets forth the services to be provided by [Contractor Name], hereinafter referred to as the "Contractor," for the California Health and Human Services Agency, Office of Technology and Solutions Integration, hereinafter referred to as the "CalHHS OTSI" or the "State."

The Agreement shall incorporate the following terms and conditions.

IT General Provisions – Cloud Computing Services (Revised and Effective 02/20/2025) published at: https://www.dgs.ca.gov/%7E/media/Divisions/PD/Acquisitions/Solicitation-Document-Attachments/IT-General-Provisions-Cloud-DGS-PD-402ITGP-Revised-02202025.pdf

2. TERM

A. The term of this Agreement shall commence on August 9, 2026, or the date the software is received by the State, and continue through August 8, 2027, or twelve (12) months.

B. The State reserves the option to amend this Agreement to increase the quantity or extend the term at the originally agreed-upon rates specified in this Agreement.

3. COST

The total cost of this Agreement is [Agreement Cost $Dollar Value]. Cost details are located in the attached, Contractor's Quote.

4. SCOPE OF SERVICES

Details of the services are provided in the attached, Contractor's Quote.

5. INVOICING AND PAYMENT PROVISIONS

A. Invoicing and Payment

1) For services satisfactorily rendered, and upon receipt and approval of the invoice(s), the CalHHS OTSI agrees to compensate Contractor in accordance with the costs set forth in the attached, Contractor's Quote.

2) Payment for software licenses shall be made in one (1) year increments and may be invoiced upon delivery of the initial services and annually thereafter.

3) Payment shall be made in accordance with the State of California's Prompt Payment Act (Government Code Section 927 et seq.).

4) Invoices may be submitted electronically via email or by mail.

a) Invoices submitted electronically shall be emailed to: AccountsPayable@otsi.ca.gov. Electronic submissions must:

(i) Be submitted individually. CalHHS OTSI will not accept multiple invoices submitted in a single email.

(ii) Contain the following in the Subject line:

- Company name
- Agreement number 75350775 and PO number (0531-####)
- Invoice number

(iii) Be in PDF format and include all of the supporting documentation as required in this Agreement.

b) Invoices submitted by mail shall be sent directly to the following address. Hard copies must include all the supporting documentation as required in this Agreement.

CalHHS Office of Technology and Solutions Integration
Attn: Accounting Office
2870 Gateway Oaks Drive, Suite 150
Sacramento, CA 95833

B. Travel and Reimbursement

The State will not be reimbursing for any travel as part of this Agreement.

C. Termination for Non-Appropriation of Federal Funds

1) It is mutually understood between the parties that this Agreement may have been written before ascertaining the availability of Congressional appropriation of funds, for the mutual benefit of both parties, in order to avoid program and fiscal delays which would occur if the Agreement were executed after that determination was made.

2) This Agreement is valid and enforceable only if sufficient funds are made available to the State by the United States Government for the term of this Agreement for the purposes of this program. In addition, this Agreement is subject to any additional restrictions, limitations, or conditions enacted by the Congress or any statute enacted by the Congress which may affect the provisions, terms, or funding of this Agreement in any manner.

3) If the Congress does not appropriate sufficient funds for the program, the State shall have the option to terminate this Agreement pursuant to this section with

thirty (30) days prior written notice or amend this Agreement to reflect any reduction in funds.

6. STATE CONTACTS

Inquiries or updates related to the software account or licenses	
Name:	Jimmie Ramos
Email Address:	Jimmie.ramos@otsi.ca.gov

Inquiries related to the PO and payments	
Email Address:	cwdspurchasing@otsi.ca.gov

7. ELECTRONIC SIGNATURES

This Agreement may be executed in any number of counterparts, each of which will be an original, but all of which together will constitute one instrument. Each party of this Agreement agrees to the use of electronic signatures, such as digital signatures that meet the requirements of the California Uniform Electronic Transactions Act (("CUETA") Cal. Civ. Code Sections 1633.1 to 1633.17), for executing this Agreement. The parties further agree that the electronic signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record pursuant to the CUETA as amended from time to time. The CUETA authorizes use of an electronic signature for transactions and contracts among parties in California, including a government agency. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the parties. For purposes of this section, a digital signature is a type of "electronic signature" as defined in subdivision (h) of Section 1633.2 of the Civil Code.

EXHIBIT A – ATTACHMENT 1
CALHHS OTSI SPECIAL PROVISIONS – PRIVACY AND SECURITY CONTROLS
(REVISED AND EFFECTIVE 11/17/2025)

1. DEFINITIONS

For purposes of this Exhibit, the term "State Data" is defined as set forth in the General Provisions.

2. CONTRACTOR RESPONSIBILITIES

A. All Contractor staff shall annually complete information privacy and security awareness training. The training shall cover, at a minimum, the following topics: phishing, threats, passwords, online/internet protections, preventative measures, and privacy as approved by the State Information Security Officer (ISO). The information privacy and security awareness training must be completed within the first two weeks of Contractor staff start date and on an annual basis thereafter, at the Contractor's expense. Each Contractor staff who receives information privacy and security training shall sign the State's certification form, indicating the staff's name and the date on which the training was completed. The Contractor staff shall provide the signed certification form to the State Contract Manager within thirty (30) days of course completion. These certifications shall be retained for a period of three (3) years following Agreement termination.

B. All Contractor staff that are or will be working with State Data shall sign the State's Confidentiality and Non-Disclosure Agreement prior to having access to State Data. The Contractor shall retain each staff's written confidentiality statement for the CalHHS OTSI inspection for a period of three (3) years following Agreement termination.

C. Prior to the commencement of work by Contractor's staff, the Contractor shall: (1) conduct a thorough background check of each proposed staff, (2) evaluate the results, and (3) certify in writing to the State Contract Manager, within 15 business days of Agreement execution (or immediately following the addition of new staff), that there is no indication that the proposed staff may present a risk to the security or integrity of the State's information technology systems or the data residing therein. The Contractor shall retain each staff's background check documentation for a period of three (3) years following Agreement termination. If, during the term of the Agreement, the Contractor becomes aware of new or previously unknown information which may impact the staff's suitability for the position, the Contractor shall immediately notify the State Contract Manager.

D. All Contractor or Contractor staff-owned or managed electronic computing devices, smart phones, tablets, personal computers, laptops, removable media storage devices, and/or similar devices (hereinafter collectively referred to as "Computing Devices"), if allowed (which permission shall be in writing), by the State Contract Manager, shall comply with the following requirements, as applicable:

i. Contractor is responsible for encryption and access control, unless otherwise set forth in the Statement of Work.

ii. Only the minimum necessary amount of State Data may be downloaded to Computing Devices, and only when absolutely necessary for current business purposes and when pre-approved in writing by the State Contract Manager.

iii. Provide an automatic timeout after no more than 10 minutes of inactivity on all Computing Devices.

iv. Any Computing Device that creates, receives, maintains, uses, or transmits State Data shall display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users shall be unable to log on to the system if they do not agree with these requirements.

v. Log successes and failures of user authentication at all layers, when accessing State assets. Maintain logs for a minimum period of 365 days. Provide access to all logs to the ISO within 30 days of request.

vi. Log all system administrator/developer access and changes if processing and/or storing State Data. Maintain logs for a minimum period of 365 days. Provide access to all logs to the ISO within 30 days of request.

vii. Log all user transactions if accessing, processing and/or storing State Data. Maintain logs for a minimum period of 365 days. Provide access to all logs to the ISO within 30 days of request.

viii. Use role-based access controls for all user authentications, enforcing the principle of Least Privilege as defined in SIMM 5300.

ix. All systems that are accessible via the Internet or store State Data shall actively use a comprehensive third-party real-time host-based intrusion detection and prevention solution that is required to be kept up to date with threat protections. Maintain logs that document compliance with this requirement and any detected threats for a minimum period of 365 days. Provide access to all logs to the ISO within 30 days after request.

x. All systems processing and/or storing State Data shall maintain and follow a process to review system logs for unauthorized access. Maintain logs that document compliance with this requirement to review system logs for a minimum period of 365 days. Provide access to all logs to the ISO within 30 days after request.

xi. All systems processing and/or storing State Data shall have a commercial third-party anti-virus software solution with a minimum daily automatic update.

xii. All users must be issued a unique username. Passwords shall not be shared. All passwords shall conform to the latest version of the CalHHS OTSI Password Standard.

xiii. Any access to State Data must be executed over an encrypted method approved by the ISO. All access shall be limited to minimum necessary and conform to the principle of Least Privilege as defined in SIMM 5300. Remote access shall meet security standards as defined in SAM 5360.1 and SIMM 5360-A, including use of a multi-factor authentication solution approved by the ISO.

xiv. All systems processing and/or storing State Data must have a documented change control procedure that assures separation of duties and protects the confidentiality, integrity, and availability of data.

E. The Contractor shall also comply with the following requirements with respect to State Data:

i. State Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, or desk. Unattended means that information is not being observed by an employee authorized to access the information. State Data in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

ii. Visitors to areas where State Data is contained shall be escorted and the visit shall be logged. State Data shall be kept out of sight while visitors are in the area.

iii. State Data shall not be removed from the premises of the Contractor except with express written permission of the CalHHS OTSI.

iv. Fax numbers shall be verified with the intended recipient before sending faxes containing State Data. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Contractor fax machines shall be located in secure areas, per SAM 5365.1.

v. State Data shall only be mailed using secure methods approved by the ISO. Large volume mailings of State Data shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail shall be encrypted with the CalHHS OTSI approved solution.

vi. State Data shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A. When transmitting State Data, all data transmissions must be encrypted end-to-end in conformance with FIPS PUB 140-3.

vii. Destruction of State Data shall be in compliance with Section 21.2.1 of the General Provisions, including, but not limited to, the standards for data destruction set forth in National Institute of Standards and Technology (NIST) 800-88, and if applicable, Section 21.12 of the General Provisions. Once State Data has been destroyed, the Contractor shall provide the State with a certificate of destruction verifying that State Data has been destroyed in accordance with the requirements of this Agreement.

F. The Contractor shall designate a security officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with the CalHHS OTSI. All exception and exemption requests shall be reviewed by the Contractor's security officer prior to submission to the ISO.

G. Security testing and remediation must be performed prior to production use of software, including new releases. Vulnerabilities that cannot be remediated prior to production must be documented in writing, including a risk assessment identifying the business impact of the identified risk(s), and submitted to the ISO within 24 hours of discovery. Written approval by the ISO is required before production use of software with known vulnerabilities is permitted.

H. Appropriate Contractor sanctions must be applied against Contractor staff who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

3. CONTACT INFORMATION

The contact information for the state contacts referenced herein are set forth below. The CalHHS OTSI reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

State Contact	State Privacy Officer	State Information Security Officer
See the SOW for State Contact information	Privacy Officer CalHHS OTSI Information Security Office CalHHS Office of Technology and Solutions Integration 2870 Gateway Oaks Drive, Suite 150 Sacramento, CA 95833 Email: privacy@otsi.ca.gov Telephone: (916) 263-0330	Information Security Officer CalHHS OTSI Information Security Office CalHHS Office of Technology and Solutions Integration 2870 Gateway Oaks Drive, Suite 150 Sacramento, CA 95833 Email: cwdsinfosec@otsi.ca.gov and otsiinfosecurity@otsi.ca.gov Telephone: (916) 263-0481

4. EXCEPTION PROCESS

The Contractor may request an exception from a requirement of this Exhibit, where compliance is not feasible or is technically impossible, or if deviation from the requirement is necessary to support a business function.

A. Any request for an exception shall be submitted in writing to the State Contract Manager from the Contractor's designated security contact.

B. Exceptions must be approved in writing by the State Contract Manager and the CalHHS OTSI ISO.

C. The term of any approved exception may not exceed twelve (12) months or as otherwise specified in the State's approval letter.

5. SURVIVAL

The provisions of this Exhibit A – Attachment 1, CalHHS OTSI Special Provisions - Privacy and Security Controls (Revised and Effective 11/17/2025) shall survive the expiration or termination of this Agreement.