California Housing Finance Agency

Request for Proposals – Remediation of Findings from Information Security Program Audit *(September 10, 2024)*

I. Background:

The California Housing Finance Agency (the "***Agency***" or "***CalHFA***") is a public instrumentality and a political subdivision of the State of California created in 1975 for the primary purpose of meeting the housing needs of persons and families of low or moderate income. The Agency provides financing and programs to create affordable single family and multifamily housing. CalHFA's governing statutes can be found in the California Health & Safety Code, Division 31, commencing at Section 50900. Additional information about the Agency is available at http://www.calhfa.ca.gov.

The Agency is soliciting statements of proposals from organizations to assist in the remediation of findings from California's Information Security Program Audit (ISPA).

II. Purpose:

The purpose of this Request for Proposals ("***RFP***") is to obtain statements of proposals from organizations interested in assisting in the remediation of findings from California's Information Security Program Audit (ISPA). Qualified organizations will have expertise in the requirements of California's State Administrative Manual (SAM) Chapter 5300, and NIST 800-53. Selected organizations must execute a contract with the Agency. The actual selection and hiring of an organization(s) may be shortly after the Agency's receipt of statements of proposals, or as need arises.

III. Qualifications:

The Agency is seeking qualifications from organizations that have demonstrated expertise in the following areas:

- California's Information Security Program Audit
- California's State Administrative Manual (SAM)
- NIST 800-53
- Working and producing artifacts to support the remediation efforts of an ISPA audit and/or any NIST related audit.

IV. Scope of Services:

A. Volume of work. The Agency is requesting assistance is remediating ten findings from the Information Security Program Audit over the next eight months.

B. Nature of Work. The Agency is seeking to contract with an organization to provide the following services:

1. Asset Management Procedures

a. Update existing asset management procedures for physical devices inventory to include the following additional inventory elements as required by SAM 5305.5:
    i. Classification of information records for 10 divisions.
    ii. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).
    iii. Importance of information assets to the execution of CalHFA's mission and program function.
    iv. Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.

2. **System Categorization per FIPS Publication 199**
    a. Utilize FIPS Publication 199 to categorize mission critical and information systems and determine the level of protection based on the information system security categorization process. This will include 13 mission critical systems, ≈450 physical devices, and ≈100 applications.
3. **System Classification**
    a. Review and document the classification of all information assets as either public or confidential according to SIMM 5305-A (including information assets residing in AWS and Azure). This will include ≈150 information assets.
4. **Document deficiencies identified through PIAs or SIMM 5310-C Evaluation**
    a. Enhance Privacy Program by establishing the following:
        i. Use SIMM 5310-C or an equivalent PTA/PIA tool to evaluate six areas: Privacy Program Administration; Collection; Use; Maintenance and Storage; Disclose/Share; Destruction/Disposal
5. **Privacy Threshold Assessments (PTAs) and Privacy Impact Assessments (PIAs)**
    a. Comply with PTA and PIA requirements by instituting the following:
        i. Establish an enterprise policy and process that explicitly describes the applicability of privacy policy to enterprise business processes and ensures compliance with the CA Information Practices Act.
        ii. Perform Privacy Threshold Assessments (PTAs) and if necessary, Privacy Impact Assessments (PIAs) upon the development or procurement of a new information system, and when proposing changes to an existing system that collect, use, maintain, store, share, disclose, or dispose of personal information.
        iii. Maintain a record of PTAs and PIAs conducted to include:
            1. System name
            2. Process project or program assessed
            3. Date the assessment was completed
            4. Names and contact information of the privacy coordinator and the information owner or project manager
6. **Key performance indicators (KPIs)**

a. Develop KPIs to measure the effectiveness of CalHFA's information security and privacy program and improve the program based on the indicators.

7. **Audit and Accountability procedures**
    a. Develop fully documented auditing and accountability procedures that provide step-by-step processes on how to perform the information security related audit review. Procedures should be expanded to monitoring and analysis of account usage, remote access, mobile device connection, configuration settings, physical access, temperature and humidity, equipment delivery and removal, use of mobile code, etc., and reporting of anomalies.
8. **Risk Assessment Policy**
    a. Develop a policy that outlines the approach for identifying, assessing, and managing risks that could potentially impact information security. Include methods for evaluating the likelihood and impact of risks, prioritizing them, and developing strategies to mitigate them.
9. **Security Assessment and Authorization Procedures**
    a. Develop procedures that outline the process for assessing the security measures in place and authorizing operations based on their compliance with security requirements.
10. **Security Planning Procedures**
    a. Establish and refine existing security planning procedures to include the steps for planning and implementing security measures within the CalHFA. Should include risk assessment, selection of security controls, and the process for reviewing and updating the security plan.

C. Deliverables. All deliverables must be reviewed and approved as complete by the California Department of Technology before being considered finalized.

V. Proposal:

The above-mentioned scope must be completed by June 1, 2025. The Statement of Proposal must include the information listed below. CalHFA appreciates your time and interest in responding to this RFP and encourages straightforward and concise responses. Responding parties should carefully note the matters provided for in Section VII, "Selection".

A. Summary of Firm.

Please provide (by narrative or attachment) a descriptive summary of your organization, including how long it has been in existence and its scope of business. Indicate if your organization qualifies as a Small Business Enterprise (SBE) and/or a Disabled Veterans Business Enterprise (DVBE) and is certified as such by the California Department of General Services. Describe how your organization is organized with respect to serving the Agency and provide a brief organizational chart with titles and names.

B. Scope of Proposal.

Please include any and all costs and fees associated with your services, including but not limited to a breakdown of cost of each service.

C. Insurance.

Please delineate insurance policies (*i.e.*, malpractice, securities transactions, workers compensation, comprehensive commercial liability, etc.) held by the organization including dollar amount and liability limits. Please provide copies of the applicable insurance declarations pages.

D. Personnel.

Please identify the personnel who you anticipate would be providing services to the Agency. Provide a brief description of the relevant experience of each individual, the role each individual will fill, his or her title, location, telephone number and the percentage of the organization's total effort that will be provided by that individual. Alternatively, you may attach resumes, as long as the additional information requested here regarding personnel, is also included in your response.

E. List of Transactions/Clients.

If applicable, please provide a list of specific matters, transactions or projects handled by each qualified personnel that may be relevant to the decision making of the Agency.

F. Value-Added Services.

To the extent not already covered, please discuss your organization’s relevant experience or special expertise that would enable you to bring value to this Agency and set your organization apart from others.

Briefly discuss an example or two of particularly innovative or helpful ways you have provided added value to clients, e.g., by providing training to the client’s staff, or by having available other services related to the services to be provided.

G. References.

Please provide several references for which your organization has performed similar work, including a summary of the services provided. References from both public agencies and private sector transaction participants are encouraged.

H. Fees.

Please provide a proposed fee arrangement and structure for your organization's services, including hourly rates, if applicable. You may also propose more than one fee structure alternative. If you propose a fee arrangement based on business volume please explain in detail how such fees would be calculated and which

types of services would or would not be covered. Please identify any fees associated with optional tasks or value-added services separately.

I. Schedule.

Please provide a detailed project schedule delineating all key project milestones and junctures, including milestones for Agency-provided information and guidance to ensure that the Project remains on time and on budget.

J. Legal Proceedings.

Identify and describe any pending legal proceeding against your organization or an officer of your organization alleging, or any judgments within the last three (3) years involving, violations of law in connection with an offering of any services.

K. Conflict of Interest.

If the organization is representing a client in civil litigation in which the State is, or may become, an adverse party, please identify and describe each such action. In addition, describe any existing or potential conflict of interest arising from your relations with, or representations of, other parties that should be considered as a factor in determining your objectivity. Provide sufficient facts, legal implications, and possible effects in order for the Agency to appreciate the significance of each potential conflict and to determine whether such conflict may disqualify the firm.

Prior to commencement of any services under a contract, your firm's employees and agents, as determined by the Agency, shall complete a California FPPC Form 700, Statement of Economic Interests as required by the Agency's Conflict of Interest Code under Section 81000 *et seq.* of the California Government Code, as well as California State Ethics Training. For further information on these requirements, see http://www.fppc.ca.gov/ and for specifics on financial disclosure http://www.fppc.ca.gov/Form700.html. If you have further questions in these regards you may also contact Sierra Grandbois at CalHFA at sgrandbois@calhfa.ca.gov. Direct, electronic filing of ethics training and certification and Form 700 are available.

L. Delivery of Statement of Proposals.

Statements of Proposals must be submitted electronically no later than **5:00 PM (PDT) on September 27, 2024** to: rnakao@calhfa.ca.gov

All materials submitted in accordance with this solicitation become the property of the California Housing Finance Agency and will not be returned. The material will be a public record subject to the disclosure provisions of the Public Records Act (Government Code Section 6250 *et seq.*). Questions concerning this Request for Proposals should be directed to rnakao@calhfa.ca.gov. When sending questions, please provide contact information and the best times for a telephone call to discuss.

VI. Selection:

The qualifications of organizations responding to this solicitation will initially be considered by staff of CalHFA. As part of the evaluation process, the Agency may request oral or telephonic interviews with the organizations and individuals being considered.

The staff will consider the following criteria:

Breadth and depth of experience and expertise in the areas described in Section III.

Ability to provide the services described in Section IV.

Timeline to provide the services described in Section IV.

Information and responses provided to requests in Section V.

Fees quoted.

Selection of an organization(s) will be an ongoing process as contracts with existing organizations expire, or specific services are needed. Consequently, the Agency understands that fees quoted at the time of this process might not still be valid. Once selected, organizations will be expected to enter into one-year to three–year contracts depending on the nature of services to be provided.

VII. Reservations:

All costs for developing and submitting the Request for Proposals pursuant to this solicitation are solely the responsibility of the respondent and shall not be reimbursable by the Agency. Although the Agency has chosen at this time to seek an RFP for services, it is not required to procure any of its contracts by way of competitive bidding and is generally not subject to many of the restrictions or requirements typically associated with State contracting practices. Accordingly, the Agency reserves its right to select one or more, or reject all, organizations responding pursuant to this solicitation.

In addition, the Agency reserves the right to:

A. Request an oral or telephonic interview with, and to require additional information from, any organization prior to its selection;

B. Select for contract negotiation the organization(s) that, in the Agency's judgment, will best meet the Agency's needs, regardless of any differences in estimated costs;

C Consider information about an organization in addition to information submitted in or obtained through oral or telephonic interviews;

D. Select one or more responding organizations other than those responding;

E. Require additional information from any respondent;

F. Terminate this process at any time without selecting any organization;

G. Change any deadline or date provided herein without notice; or

H. Otherwise amend or modify any of the terms or provisions of this solicitation.

VIII. Statement of Proposals Material:

All material submitted in accordance with this RFP become the property of CalHFA, and will not be returned. The material will be a public record subject to the disclosure provisions of the California Public Records Act (Government Code Section 6250 et seq.). Applicants should be aware that marking a document "confidential" or "proprietary" in a Statement of Proposals may not keep that document from being released after final selection.

If CalHFA receives a Public Records Act request that may include confidential information of the submitting organization, and CalHFA determines that such records are not exempt from public disclosure, CalHFA will make reasonable efforts to provide written notice to the organization prior to releasing such information. Such an organization may seek relief in court to enjoin the disclosure of such confidential information, but shall have no other rights or remedies against CalHFA in connection with the disclosure of such information.