REQUEST FOR PROPOSALS

Penetration Testing Services

Posting Date: January 20th, 2023
Response Submission Deadline: 3:00 EST p.m. on February 16th, 2023.

NOTE TO RESPONDENTS:

Please be advised that **all** submissions (including those not selected for engagement) may be made available to the public on request pursuant to the Rhode Island Access to Public Records Act, Chapter 2 of Title 38 of the Rhode Island General Laws (the "APRA") upon award of a contract(s). As a result, respondents are advised not to include information that they deem proprietary or confidential or that constitutes a trade secret.

INTRODUCTION

Through this Request for Proposals ("RFP"), the Rhode Island Housing and Mortgage Finance Corporation ("RIHousing") seeks proposals from qualified firms to perform penetration tests of its network, applications, and buildings over a two (2)-year period, with an option to extend for an additional two (2)-year period, as further defined in Attachment A.

INSTRUCTIONS

Proposals must be submitted via email to: **Carl Rotella, Director of Information Technology at crotella@rihousing.com** no later than the response submission deadline set forth above. Please also direct a courtesy copy by email to: **Nathaniel Borrero, Senior Security Engineer** at **nborrero@rihousing.com**.

Proposals that are not received by the response submission deadline or that do not adhere to the submission instructions described herein shall not be accepted or considered by RIHousing.

Proposals should be concise and adhere to the word count applicable to each section of this Request for Proposals ("RFP"). Proposals should be presented on business letterhead and include all attachments, certifications (including the Submissions Certification at Attachment A), and work samples (as applicable). Please note that failure to provide any information, certification, or document requested in this RFP may cause your submission not to be reviewed or considered by RIHousing.

RIHousing may invite one or more finalists to make presentations, including demonstrations of requested products, if applicable.

SCOPE OF WORK

Please see the Scope of Work as provided on Attachment B.

ITEMS TO BE INCLUDED WITH YOUR PROPOSAL

Section A: General Firm Information (Total word limit: 500 words)

SUBMISSION CHECK LIST

☐ 1. Provide a brief description of your firm, including but not limited to the following:

a. Name of the principal(s) of the firm.
b. Name, business telephone number and business email address of a representative of the firm authorized to discuss your proposal.
c. Locations of all offices of the firm.
d. Number of employees of the firm.

RIHousing requests that the contact information provided in response to this subsection (1) be strictly limited to business addresses, telephone numbers, and email addresses to protect any personal information from being made available to the public pursuant to APRA.

Section B: Experience and Resources (Total word limit: 3500 words)

☐ 1. Describe your firm and its capabilities. In particular, support your capacity to perform the Scope of Work.

☐ 2. Indicate which principals and associates from your firm would be involved in providing services to RIHousing. Provide appropriate background information for each such person and identify their responsibilities.

☐ 3. Provide a detailed list of references, including a contact name and business telephone number for organizations or businesses for whom you have performed similar work.

☐ 4. Describe your firm's information security systems and the steps that your firm takes to safeguard client communication, confidential information, and client data. Include in your response whether your firm performs penetration testing, your firm's encryption methods, and whether client data is stored onshore or offshore.

Section C: Fee Structure (Total word limit: 500 words)

The cost of services is one of the factors that will be considered in awarding this contract. The information requested in this section is required to support the reasonableness of your fees.

☐ 1. Please provide a cost proposal for providing the Scope of Work at Attachment B. RIHousing anticipates a 2-year agreement with four (4) separate tests occurring at six (6) month intervals and one on-site physical penetration test in the two (2) year period. Please provide pricing broken out for each test.

☐ 2. Provide an itemized breakdown of billing rates and hourly costs, list of key personnel and their hourly rates, reimbursable expenses, etc. for any services that may be requested in addition to the services previously described.

☐ 3. Please provide any other fee information applicable to the engagement that has not been previously covered that you wish to bring to the attention of RIHousing.

Section D: Affirmative Action Plan and Minority Owned Business/Women Owned Business

☐ 1. RIHousing encourages the participation of persons of color, women, persons with disabilities and members of other federally and State-protected classes. Describe your firm's affirmative action program and activities. Include the number and percentage of members of federally and State-protected classes who are either principals or senior managers in your firm, the number and percentage of members of federally and State-protected classes in your firm who will work on RIHousing's engagement and, if applicable, a copy of your Minority- or Women-Owned Business Enterprise state certification.

Section E: Miscellaneous (Total word limit: 1000 words)

☐ 1. Discuss any topics not covered in this RFP that you would like to bring to RIHousing's attention.

Section F. Certifications

☐ All applicants must respond to and provide documentation as outlined in the Request for Proposals Submission Certifications at Attachment A.

EVALUATION AND SELECTION

A selection committee consisting of RIHousing employees will review all proposals that meet the requirements set forth in the "Instructions" section of this RFP and make a selection based on the following factors:

- Professional capacity to undertake the Scope of Work (as evaluated by reference in Section B: Experience and Resources);
- Proposed fee structure (as evaluated by reference in Section C: Fee Structure);
- Ability to perform within time and budget constraints (as evaluated by reference in Section B);
- Evaluation of proposed project approach (as contained in the Attachment B-Scope of Work. Section B);
- Previous work experience and performance with RIHousing and/or similar organizations (as provided in Section B: Experience and Resources, subsection 3);
- Recommendations by references (as provided in Section B: Experience and Resources, subsection 3);
- Firm minority status and affirmative action program or activities (as requested in Section D: Affirmative Action Plan and Minority Owned Business/Women Owned Business)
- Other pertinent information submitted.

By this RFP, RIHousing has not committed itself to undertake the work set forth herein. RIHousing reserves the right to reject any and all proposals, to rebid the original or amended scope of services and to enter into negotiations with one or more respondents. RIHousing reserves the right to make those decisions after its receipt of responses. RIHousing's decision on these matters is final.

For additional information contact: **Carl Rotella, Director of Information Technology at crotella@rihousing.com.**

Attachment A

Requests for Proposals Submission Certifications

Please respond to **all** items below and include it in your response to this RFP. Be sure to include any additional information in the space provided or as an attachment as needed. Please ensure that any attachments refer to the appropriate item by name (i.e., "Conflict of Interest," "Major State Decision Maker," etc.)

Total word limit for Sections A and B: 500 words

Section A: Conflicts of Interest

1. Identify any conflict of interest that may arise as a result of business activities or ventures by your firm and associates of your firm, employees, or subcontractors as a result of any individual's status as a member of the board of directors of any organization likely to interact with RIHousing. **If none, check below**.

   ☐ None

2. Describe how your firm will handle actual and or potential conflicts of interest *(please include in your proposal or attach a sheet with this information).*

Section B: Litigation, Proceedings, Investigations

1. Identify any material litigation, administrative proceedings, or investigations in which your firm is currently involved. **If none, check below.**

   ☐ None

2. Identify any material litigation, administrative proceedings, or investigations to which your firm or any of its principals, partners, associates, subcontractors, or support staff was a party, that has been finally adjudicated or settled within the past two (2) years. **If none, check below.**

   ☐ None

Section C: Certifications

1. RIHousing insists upon full compliance with Chapter 27 of Title 17 of the Rhode Island General Laws, Reporting of Political Contributions by State Vendors. This law requires State Vendors entering into contracts to provide services to an agency such as RIHousing, for the aggregate sum of $5,000 or more, to file an affidavit with the State Board of Elections

concerning reportable political contributions. The affidavit must state whether the State Vendor (and any related parties as defined in the law) has, within 24 months preceding the date of the contract, contributed an aggregate amount in excess of $250 within a calendar year to any general officer, any candidate for general office, or any political party. **Please acknowledge your understanding below.**

☐ I have read and understand the requirements of Chapter 27 of Title 17 of the Rhode Island General Laws, Reporting of Political Contributions by State Vendors.

2. Does any Rhode Island "Major State Decision-maker," as defined below, or the spouse or dependent child of such person, hold (i) a ten percent or greater equity interest, or (ii) a Five Thousand Dollar or greater cash interest in this business?

   For purposes of this question, "Major State Decision-maker" means:

   (i) All general officers; and all executive or administrative head or heads of any state executive agency enumerated in § 42-6-1 as well as the executive or administrative head or heads of state quasi-public corporations, whether appointed or serving as an employee. The phrase "executive or administrative head or heads" shall include anyone serving in the positions of director, executive director, deputy director, assistant director, executive counsel, or chief of staff;

   (ii) All members of the general assembly and the executive or administrative head or heads of a state legislative agency, whether appointed or serving as an employee. The phrase "executive or administrative head or heads" shall include anyone serving in the positions of director, executive director, deputy director, assistant director, executive counsel, or chief of staff;

   (iii) All members of the state judiciary and all state magistrates and the executive or administrative head or heads of a state judicial agency, whether appointed or serving as an employee. The phrase "executive or administrative head or heads" shall include anyone serving in the positions of director, executive director, deputy director, assistant director, executive counsel, chief of staff or state court administrator.

   Please indicate your response below.

   ☐ Yes

   If your answer is "Yes," please identify the Major State Decision-maker, specify the nature of their ownership interest, and provide a copy of the annual financial disclosure required to be filed with the Rhode Island Ethics Commission pursuant to R.I.G.L. §§36-14-16, 17 and 18.

   ☐ No

3. In the course of providing goods or services to RIHousing, the selected respondent may receive certain personal information specific to RIHousing customer(s) including, without limitation, customer names and addresses, telephone numbers, email addresses, dates of birth, loan numbers, account numbers, social security numbers, driver's license or identification card numbers, employment and income information, photographic likenesses, tax returns, or other personal or financial information (hereinafter collectively referred to as the "Personal Information"). The maintenance of the Personal Information in strict confidence and the confinement of its use to RIHousing are of vital importance to RIHousing.

Please certify below that in the event your firm is selected:

(i) any Personal Information disclosed to your firm by RIHousing or which your firm acquires as a result of it services hereunder will be regarded by your firm as confidential, and shall not be copied or disclosed to any third party, unless RIHousing has given its prior written consent thereto; and

(ii) your firm agrees to take all reasonable measures to (a) ensure the security and confidentiality of the Personal Information, (b) protect against any anticipated threats or hazards to the security or integrity of the Personal Information, and (c) maintain reasonable security procedures and practices appropriate to your firm's size, the nature of the Personal Information, and the purpose for which the Personal Information was collected in order to protect the Personal Information from unauthorized access, use, modification, destruction or disclosure; and

(iii) when discarding the Personal Information, destroying it in a commercially reasonable manner such that no third party can view or recreate the information, electronically or otherwise.

These provisions, which implement the requirements of the Rhode Island Identity Theft Protection Act, R.I.G.L. § 11-49.2 et seq., will also be incorporated into the final contract with the selected respondent(s). In addition, if selected, your firm may be requested to provide a copy of its information security plan.

☐ I certify that in the event our firm is selected, we will comply with the Personal Information and Security guidelines noted above.

Your firm's president, chairman or CEO must certify below that (i) no member of your firm has made inquiries or contacts with respect to this RFP other than in an email or written communication to **Carl Rotella, Director of Information Technology at** crotella@rihousing.com seeking clarification on the Scope of Work set forth in this proposal, from the date of this RFP through the date of your proposal, (ii) no member of your firm will make any such inquiry or contact until after **February 16, 2023**, (iii) all information in the proposal is true and correct to the best of your knowledge, (iv) no member of your firm gave anything of monetary value or promise of future employment to a RIHousing employee or Commissioner, or a relative of the same, based on any understanding that

such person's action or judgment will be influenced, and (v) your firm is in full compliance with Chapter 27 of Title 17 of the Rhode Island General Laws, Reporting of Political Contributions by State Vendors.

☐ I certify that no member of our firm has made or will make any such inquiries or contacts; all information supplied is true and correct; no member of our firm has provided anything of value to influence RIHousing; and our firm is in compliance with applicable political contribution reporting.

President, Chairman or CEO *(print):* _____

Signature: _____

Firm Name:_____

Attachment B

Scope of Work

I. Services to be Provided

RIHousing is soliciting proposals from qualified vendors to perform four (4) penetration tests of RIHousing's network, applications, and one (1) on-site physical penetration test, over a two (2)-year period for purposes of identifying and documenting risk and vulnerabilities and for compliance and auditing purposes. At RIHousing's option, there may be an option to extend the contract for an additional two (2) years.

At a minimum, the penetration test should include the following tactics, techniques, and procedures:

- Social engineering (including phishing and vishing)
- Web application testing (credentialed and non-credentialed)
- Physical penetration testing (one (1) physical location) in Providence, RI
- External network penetration testing
- Wireless security testing

II. Project Schedule

Four (4) separate tests shall occur at six (6)-month intervals. The first test shall occur in May 2023. The second test will occur in November 2023. The third test shall occur in May of 2024, and the fourth test shall occur in November 2024. Any changes to this schedule are subject to approval of RIHousing.

One (1) physical penetration test on site at RIHousing's building in 2024 at a time and date to be determined in coordination with RIHousing.

III. Project Approach

The vendor shall perform penetration tests both remotely and on site. Physical access to RIHousing property and network will be permitted in writing prior to the test. The vendor will be required to receive approval from RIHousing before the testing window.

The scope of the test will include approximately three hundred (300) public IP addresses, five (5) wildcard domains, five (5) web applications, and one (1) physical location in Providence,

RI. RIHousing reserves the right to add or remove IP's, domains, or applications to the scope as our network expands or contracts.

Throughout the engagement, vulnerabilities will be identified and documented. The vendor shall promptly notify Carl Rotella, Director of Information Technology at 401-457-1240 or crotella@rihousing.com in the event of a compromised application or critical risk finding.

The vendor will deliver a final report to RIHousing within five (5) business days of completing the final pen testing.

The final report shall include the following deliverables:

- Vulnerabilities identified throughout the engagement to include discovered network and application entry points, user accounts, open network services, and visible hostnames.
- For potential and proven exploits, the report shall include a description of attack methodology used.
- For physical location, the report shall include a description and photos (including locations) of vulnerable access points, gaps in security, and internal risks.
- Recommended remediation and temporary mitigations, if applicable.

Upon delivery of the final report, the vendor will participate in a review call with RIHousing's Information Security team to discuss discovered vulnerabilities and recommendations.

RIHousing will submit questions regarding the report in writing to the vendor within fourteen (14) calendar days of the report's delivery for review and response. The vendor shall provide an answer to questions within three (3) days of receipt.

IV. Budget and Payment Terms

Vendor payment shall be made within thirty (30) days of delivery of final report.