**Request for Proposals**
**Penetration Testing of**
**Network and Web Applications**

## 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 and web applications over a two (2)-year period as further defined in Attachment A.

## INSTRUCTIONS

An electronic version of the proposal should be submitted to Carl Rotella, Director of Information Technology at crotella@rihousing.com. Please also direct a courtesy copy by email to: Nathaniel Borrero at nborrero@rihousing.com. Proposals should be presented on business letterhead.

**Proposals must be received no later than 3:00 EST p.m. on Tuesday, January 12, 2021.** Responses received after this date and time shall not be accepted.

Respondents are advised that all submissions (including those not selected for engagement) may be made available to the public on request upon completion of the process and award of a contract(s).

## SCOPE OF WORK

Please see the Scope of Work provided at Attachment A.

**Submission Check List**

## ITEMS TO BE INCLUDED WITH YOUR PROPOSAL

Please note that failure to provide any information, certification, or document requested in this RFP may cause your submission not to be scored.

A. General Firm Information

☐

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, telephone number and email address of a representative of the firm authorized to discuss your proposal.
c. Address of all offices of the firm.
d. Number of employees of the firm.

B. Experience and Resources

☐ 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 his or her responsibilities.

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

☐ 4. 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, please provide a statement to such effect.**

☐ 5. Describe how your firm will handle actual and or potential conflicts of interest.

☐ 6. Identify any material litigation, administrative proceedings or investigations in which your firm is currently involved. 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, please provide a statement to such effect.**

C. Fee Structure

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 A.

2. 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.

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.

E. Miscellaneous

1. Discuss any topics not covered in this Request for Proposals that you would like to bring to RIHousing's attention.

F. 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 of this in your RFP response.

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.

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. If your answer is "No," please provide a statement to such effect.

☐

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 include a letter from your president, chairman or CEO certifying 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.

☐

4. Please include a letter from your president, chairman or CEO certifying that (i) no member of your firm has made inquiries or contacts with respect to this Request for Proposals 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 the submission of your proposal, (ii) no member of your firm will make any such inquiry or contact until after 3:00 PM on January 12, 2021, (iii) all information in your proposal is true and correct to the best of her/his 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.

## EVALUATION AND SELECTION

A selection committee consisting of RIHousing employees (the "Committee") will review all proposals and make a determination based on the following factors:

- Professional capacity to undertake the Scope of Work
- Proposed fee structure
- Ability to perform within timeframe required
- Recommendations by references
- Firm minority status and affirmative action program or activities
- Other pertinent information submitted.

By this Request for Proposals, RIHousing has not committed itself to undertake the work set forth. 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 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**

**Scope of Work**
**PENETRATION TESTING**
**OF**
**NETWORK AND WEB APPLICATIONS**

## Purpose

RIHousing is soliciting proposals from qualified vendors to perform four (4) penetration tests of RIHousing's networks over a two (2)-year period for purposes of identifying and documenting risk and vulnerabilities and for compliance and auditing purposes.

## Project Timeline

Four (4) separate tests shall occur at six (6)-month intervals. The first test shall occur in May 2021. The second test will occur in November 2021. The third test shall occur in May of 2022, and the fourth test shall occur in November 2022. Any changes to this schedule are subject to approval of RIHousing.

## Scope

The vendor shall perform penetration tests remotely. Physical access to RIHousing property and network will not be permitted. The vendor will be required to receive approval from RIHousing before the testing window. RIHousing reserves the right to add network and non-credentialed web application testing requirements for tests three (3) and four (4).

The following networks and web applications are in-scope:
*External Network Penetration Test*

- 198.7.235.0/24
- 131.109.208.160/27
- 72.196.41.152/29
- 13.92.23.145
- 104.45.176.246
- 52.191.119.200
- 52.170.166.80
- 20.62.157.180

IP whitelisting of RIHousing's public IPs.

*Non-Credentialed Web Application Testing*

- *.rihousing.com

- *.mtgservicingsolutions.com
- *.rihmfc.com
- *.rhodeislandhousing.org
- waitlist-centralri.com

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

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

*Final Report 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.
- Recommended remediation and temporary mitigations, if applicable.

*Document Review Requirements*

- Upon delivery of the final report, the vendor will participate in a review call with RIHousing's information security team to discuss discovered vulnerabilities.

- 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.