BOSTON RETIREMENT SYSTEM

Request for Proposal for Cybersecurity Professional Services

INTRODUCTION

The Boston Retirement System (hereinafter "BRS") is undertaking procurement for cybersecurity professional services. BRS seeks a qualified cybersecurity vendor with the following characteristics

- Deep cybersecurity expertise and experience
- Experience working with public sector clients
- Demonstrable ability to scale cybersecurity frameworks appropriately to BRS
- Experience with similarly situated organizations designing and conducting cyber tabletop exercises
- Competitive pricing

PROJECT SUMMARY

Professional services are requested for two specific projects

(1) review and update the BRS written incident response plan (IRP) and

2) develop and implement two (2) Homeland Security Exercise and Evaluation Program (HSEEP) compliant tabletop exercises (TTX).

The tabletop exercises (TTX) are intended to test the incident response plans and other policies while allowing participants to practice decision-making, communication under pressure, and collaborative problem-solving. Exercise One would be focused on a cyber incident that tests BRS senior management and key staff responses to an organization specific cybersecurity incident. Exercise two, which will be held later, would be broader in scope and will include detection, response, and communications activity with a number of impacted partners and stakeholders.

HIGH LEVEL SCHEDULE

RFP Issued		**January 24, 2025**
Bidders' Q&A Web Meeting[1]		**February 5, 2024**
Answers to Questions Posted		**February 7, 2025**
Responses Due		**February 14, 2025**
Vendor Selected		**February 26, 2025**
Project Kick Off		**March 10, 2025**

[1]Bidder's Web Meeting 2/5/2025 at 2:00 pm Eastern (Boston)
meet.google.com/hae-okkt-imo
Phone Numbers (US)
+1 860-969-1807
PIN: 179 861 369#

Vendor must be ready to staff what BRS expects to be a mid-March to mid-June project with all work completed by June 30, 2025.

ADDITIONAL BACKGROUND

BRS employs fewer than 50 staff overall with a commensurately small technology staff. While such lean staffing meets operational needs, expanding cybersecurity skills is daunting in terms of availability, expense, and potential turnover in the red-hot cybersecurity labor market. Yet, the agency manages approximately $6 billion in invested assets and cash, an over $60 million monthly benefits payroll, and houses extensive PII (personally identifiable information) and financial information for about 100,000 members, recipients, and deceased members.

Organizationally, the Boston Retirement System, (BRS), is considered an adjoining agency for the City of Boston. Through its location at the Boston City Hall and intertwined operations for technology and other departmental (Treasury, Group Health, etc.) services, BRS shares a risk profile with the City of Boston. In addition, there are BRS members, both employees and pension recipients, spread across other communities in the Commonwealth and the United States, and some international recipients.

BRS is subject to the oversight and regulations of the Public Employee Retirement Administration Commission ("PERAC"). BRS itself is governed by a five-member Board and serves employees and beneficiaries of employees of the City of Boston, Boston Redevelopment Authority d/b/a Boston Planning & Development Agency, Boston Public Health Commission, Boston Housing Authority, Boston Water & Sewer Commission, as well as some Suffolk County Sheriff's Department retirees

In September 2022, BRS completed a formal cybersecurity risk assessment and has addressed many of its findings. At this point, the lack of the required skills and targeted experience has limited the organization's ability to move forward in their cyber maturity. An incident response document has been developed but needs review and improvement. This unmet need involves applying expertise for response and policy documentation - a top priority - as is testing management and staff understanding and application of these documents in real world scenarios.

BRS has achieved a basic level of sustained focus, forums, and processes. For example, there are quarterly cybersecurity meetings with the CISO (Chief Information Security Officer) for City of Boston and the pension software vendor, (Vitech). These are working sessions where recent experience, threat awareness, and ongoing activity coordination comprise the agenda. In addition, the annual cybersecurity insurance process demands extensive preparation and has become a year-round background activity with an eye towards premium reduction, coverage maximization, and familiarity with the claims process in the event of an incident.

Other related initiatives include City of Boston technology group mandatory cybersecurity awareness training several times per year for all City Hall staff including BRS, as well as frequent staff phishing tests. Since January 2023 the BRS has been enrolled in the MS-ISAC - CIS Center for Internet Security.

PROFESSIONAL SERVICES REQUIRED

As introduced above, the envisioned project will update existing IRP documentation and conduct custom HSEEP compliant Tabletop Exercises. This approach allows further strengthening and provides an opportunity for BRS to test its readiness and response capabilities in the event of a cyberattack targeting vital information, investments, and critical constituent services. By simulating a realistic scenario and

engaging key stakeholders, the exercise aims to enhance the agency's resilience and preparedness in safeguarding sensitive financial information and maintaining trust with stakeholders.

A more detail view, indicates the project will include the following steps:

1. PLAN REVIEW AND UPDATE – Conduct a review of BRS's current incident response plan documentation, associated policies and roles that would be involved during an incident response. This includes making recommendations to update and improve the materials.

2. TABLETOP DESIGN AND DEVELOPMENT (Exercise one) – Work with key BRS stakeholders to develop a scenario that is realistic to BRS's technical environment, current processes, and infrastructure.

3. TABLETOP DELIVERY (Exercise one)– Using Homeland Security Exercise and Evaluation Program (HSEEP) principles, conduct tabletop exercise to be conducted at a BRS location with no more than 5-10 active BRS leadership participants (executives/Key staff) and observers (but no more than 15 people in total), assuming appropriate space. Focus on leadership-level processes, concerns, and decision-making; technical and legal elements addressed primarily through conclusory injects designed to lead to discussion/decision points. The tabletop is designed to take place over a four-hour period.

4. EXERCISE EVALUATION, FINDINGS & COMPLIANCE – Following the tabletop, prepare a report containing findings observed during the tabletop, as well as takeaways for continued consideration.

5. IMPLEMENT IMPROVEMENTS - Make necessary improvements to BRS incident response plan, processes, and procedures. Ensure that everyone involved understands the changes and is prepared for future incidents.

6. TABLETOP DEVELOPMENT (Exercise two) – Work with key BRS stakeholders to develop a broader incident scenario that is realistic to BRS's technical environment, current processes, and that of key partners and suppliers.

7. TABLETOP DELIVERY (Exercise two)– Conduct tabletop exercise to be conducted at a BRS location with key BRS participants (executives/Key staff) and critical partners – including members of outside response team, counsel, forensics, etc.) and key partners such as the City of Boston technology dept (DoIT), pension software vendor (Vitech), etc.). Focus on leadership-level processes, concerns, and decision-making; technical and legal elements addressed primarily through conclusory injects designed to lead to discussion/decision points. The tabletop is designed to take place over a four-hour period.

8. AFTER ACTION REVIEW (AAR) - Preparation of a high-level summary and After-Action Review (AAR), including potential improvement plan. Review and update BRS incident response plan based on the feedback and data collected. Analyze the results of the test to identify strengths and weaknesses, compare actual outcomes with expected outcomes, and evaluate performance. Make any necessary changes and improvements to the plan, addressing any gaps, issues, or errors discovered during the test. Incorporate any new information, best practices, or lessons learned. Finally, communicate the updated plan to team members and stakeholders, providing them with updated training and documentation to ensure they are aware of the changes and their implications.

Note that the outcomes will be TTX 1 Findings and TTX 2 After Action Review each of which constitutes a BRS acceptance milestone. The primary impact ("metric") of each includes evaluation of response and revisions to the Incident Response Plan. For each TTX, BRS will evaluate

- Effectiveness of incident detection and response
- Coordination and communication among stakeholders
- Adherence to policies, procedures, and regulatory requirements
- Ability to recover systems and services in a timely manner
- Lessons learned and areas for improvement identified during the after-action review

Minimum Meetings to support the project

Seq	Description	Count
1	Prep	1
2	Kick Off (repeated for scheduling purposes)	2
3	Incident Response Plan - Initial Feedback - Impact to TTX planning	2
4	TTX 1 Planning	2
5	TTX 1	1
6	TTX 2 Planning	2
7	TTX	1
	Minimum total meetings	11

Vendor Response Process

Respondents are cautioned to read this RFP carefully and to conform to its requirements. Failure to comply with the requirements of this RFP may serve as grounds for rejection of a submission.

Per Massachusetts procurement regulation, vendors are instructed to provide their responses in two separate documents

1. A non-price or ("technical") proposal that addresses the approach to the project
2. A price proposal indicating a total fixed price offer with breakdown of hourly rates, summary of anticipated activities, and payment terms.

The non-price portion must open with a Transmittal Letter:

> A signed letter of transmittal briefly stating the Offeror's understanding of the work to be performed, the commitment to perform the work within the time period, a statement of qualifications as to why the Offeror believes itself to be the best qualified to perform the engagement and a statement that the proposal is a firm and irrevocable offer, good for the period of the engagement.

In their responses, offerors are directed to provide a concise but complete picture of their

- Relevant experience and expertise
- Approach for staffing and delivering the work described above
- Understanding of BRS scale and cybersecurity context

Offeror must include the following Organizational Profile information:

1. Company name
2. Federal Identification Number
3. Home office address
4. Telephone
5. Address and telephone number of nearest support office
6. Name, telephone number and email address of contact person. This person must be capable of committing the Offeror to an agreement with the City
7. Number of years company has operated under this name
8. Year company was founded
9. Brief description of the nature of the company's business
10. Number of years company has been in present business

If Offeror is a corporation, state the following:

1. Where the company was incorporated
2. The names and addresses of all officers
3. Parent corporations
4. All subsidiaries

In addition, Offerors must

- Include Bios and resumes for all individuals associated with the Respondent providing the services; equivalent profiles may be substituted at a later date if agreed by BRS.
- Identify any sub-contractors expected in providing the services.

THERE SHOULD BE NO DOLLAR UNITS OR TOTAL COSTS INCLUDED IN THE TECHNICAL PROPOSAL DOCUMENT.

BRS is posting this RFP to several online venues

1. COMMBUYS Massachusetts procurement portal
2. Two web sites
    a. Boston Retirement System https://www.boston.gov/departments/retirement
    b. PERAC https://www.mass.gov/info-details/request-for-proposal-rfp-notices

The COMMBUYS portal supports upload of Offeror responses and supporting documents. If not responding via COMMBUYS or should there be any COMMBUYS complexities, Offerors are instructed to provide digital copies via email to BRS General Counsel, Natacha Thomas natacha.thomas@boston.gov

Vendor Response Evaluation and Scoring

In their response, Offerors are directed to describe a minimum of three (3) but no more than five (5) relevant projects, i.e. IRP and TTX with particular interest in client work that included both activities. The project descriptions may be brief, such as a paragraph each, and need not include the name of the

client at this time. (BRS reserves the right to know the organization described at a later point under non-disclosure terms).

In the project descriptions, BRS is looking for successful related projects. At a minimum, the project descriptions should describe the work done, the scale and general characteristics of the client, duration, and other facts the Offeror views as advantageous.

The following table shows the scoring elements and their weight that BRS will use in its evaluation.

Scoring Element	Description	Weight
Experience	Cybersecurity depth with specific IRP and TTX experience; ideally in a small public sector setting. Relevant experience of assigned team members.	40%
References	At least two (2) and no more than four (4); the associated projects should include IRP and TTX work in an organization similar to BRS.	20%
Scale	Map to a small (50-person) agency while maintaining full HSEEP compliance	20%
Submission	Quality and completeness	20%

CAVEATS

- BRS may amend, republish, or not award at its discretion
- Offerors must be willing to sign a Non-Disclosure Agreement

Submissions must include the following completed and signed contractual documents:

FORM CM06 CERTIFICATE OF AUTHORITY (FOR CORPORATIONS ONLY)

FORM CM09 CONTRACTOR CERTIFICATION

LIVING WAGE FORM 8

LIVING WAGE FORM 2

FORM CM 10-11 STANDARD CONTRACT

FORM CM 15A CORI

FORM CM 15B CORI

FORM CM 16 WAGE THEFT PREVENTION

Appendix A Required- Certification of Non-Collusion

CERTIFICATION OF NON-COLLUSION

The undersigned certifies under penalties of perjury that this bid or proposal has been made and submitted in good faith and without collusion or fraud with any other person. As used in this certification, the word "person" shall mean any natural person, business, partnership, corporation, union, committee, club or other organization, entity or group of individuals.

_____
(Signature of individual submitting bid or proposal)

_____
(Name of business)

Appendix B Required- Certificate of Tax Compliance

APPENDIX B

Certification of Compliance with Massachusetts Tax Laws pursuant to M.G.L. Ch. 62C, §49A

Under the pains and penalties of perjury, I hereby certify, as required by General Laws, Chapter 62C, Section 49A, that:

_____
Name of Corporation, Partnership
or Sole Proprietorship

has complied with all laws of the Commonwealth of Massachusetts relating to taxes, reporting of employees and contractors, and withholding and remitting child support. The successful Proposer also agrees to provide the Boston Retirement System at closing a certificate of good standing from the Massachusetts Department of Revenue.

_____
Signature

_____
Title

_____
Date