



Request for Proposal for Information Systems Risk Assessment

RFP No. 2018-001

August 1, 2018

Table of Contents

1. Summary	3
2. Background Information	4
3. Schedule of Events	5
4. Project Scope	5
5. Vendor Preferences	10
6. Proposal Preparation.....	10
6.1 Technical Proposal.....	11
6.2 Cost Proposal.....	13
7. Proposal Evaluation and Contract Award	13
8. Procurement and Contract Administration.....	14

ATTACHMENTS:

ERSRI Regulation No. 1.3, *Rules Concerning the Selection of Consultants*

1. Summary

The Employees' Retirement System of Rhode Island (ERSRI) seeks to secure a contract for an Information Systems security risk assessment audit. The purpose of this engagement is to request an independent assessment of ERSRI's operations, internal controls and its policies and procedures as well as an audit of its SaaS line of business system hosted by Morneau Shepell (MS) located in Toronto, Canada. During the course of the engagement it is expected that the firm will:

- Audit critical systems security model and workflows to identify vulnerabilities and threats.
- Conduct a physical security assessment of the premises of ERSRI and surrounding area and its Application Service Provider for benefits administration, MS in Toronto, Canada. Recommend the corrective and preventative solutions, should they be required, for ERSRI or MS to implement in an effort to improve the informational environment.
- Draft appropriate security policies and procedures.
- Enter into a contract to provide monthly on-site risk management and review of cyber security procedures, analysis of system output data to identify potential breaches, suggest best practice, apprise senior management of known threats.

Proposals must be submitted no later than the deadline detailed in Section 3, Schedule of Events. Failure to submit a proposal prior to this deadline shall disqualify it from consideration.

Interested parties shall direct all communications regarding this RFP to the RFP Administrator noted below and no other persons.

Bidders should submit their proposals to:

Mailing and Delivery Address

Frank J. Karpinski, Executive Director
Employees' Retirement System of Rhode Island
50 Service Avenue, 2nd Floor
Warwick, Rhode Island 02886

Proposals must be received by:

September 28, 2018 at 4:00 p.m.

No exceptions to this deadline will be allowed unless the Employees' Retirement System extends the deadline whereupon it will notify potential respondents to the RFP in the same manner the RFP was issued. The firm's response to this RFP shall be no more than 30 pages (exclusive of exhibits).

You must submit your original proposal in a sealed package. Clearly mark the outside of your package:

**Employees' Retirement System of Rhode Island
RFP for Internal Audit Services 2018-001**

Any firm that wishes to correct, amend or supplement their proposal must do so prior to the filing deadline and must do so by withdrawing its proposal in its entirety and submitting a complete, corrected proposal package. Modification in any other manner will not be accepted.

Proposals become the property of ERSRI upon submission and will not be returned.

All cost for developing proposals is entirely the responsibility of the firm and shall not be chargeable to ERSRI. ERSRI accepts no responsibility for lost or late delivery of proposals.

Questions about the Request for Proposal must be submitted in writing via email or by mail to the

RFP Administrator:

Frank J. Karpinski, Executive Director
Employees' Retirement System of Rhode Island
50 Service Avenue, 2nd Floor
Warwick, RI 02886

Phone: (401) 462-7610

Email: frank.karpinski@ersri.org

All questions must be received no later than **September 14, 2018 at 4:00 p.m.** and include an email address to forward responses. All questions received by this deadline will be answered in writing and sent via email. Copies of all questions and the ERSRI response will be emailed to all parties who submitted questions and or who request in writing before **September 21, 2018 at 4:00p.m.** a copy of the Q&A. This procedure will constitute the bidders conference as referenced in Rule No. 3 Concerning the Selection of Consultants, Section 1.3.2(D)(3).

Unauthorized contact regarding this RFP with employees or officials of the State of Rhode Island other than the RFP Administrator identified above may result in vendor's disqualification from this procurement process.

2. Background Information

ERSRI is a political subdivision of the State of Rhode Island that administers a public pension plan having \$8.3 billion in assets, which are managed by the State Investment Commission (SIC) and the General Treasurer's office. ERSRI consists of 30 staff members and is administered by the 15-member State of Rhode Island Retirement Board. ERSRI interrelates with other state government entities including principally the Department of Administration, the State Auditor General's Office, and the State Legislature.

ERSRI administers four (4) defined benefit pension plans:

- *Employees' Retirement System (ERS)*, established in 1936, which includes state employees and all teachers.
- *Municipal Employees' Retirement System (MERS)*, established in 1951, which includes municipal employees and local police and fire employees.
- *State Police Retirement Benefits Trust (SPRBT)* which includes state police hired after July 1, 1987.

- *Judicial Retirement Benefits Trust (JRBT)* which includes judges hired after December 31, 1989.

The four plans cover approximately 35,000 active members and 29,000 retirees and beneficiaries. ERSRI supports approximately 215 employers located throughout the State. Participating employers are required by statute to provide all data necessary for ERSRI's effective operation. The rules for ERSRI administration and plan benefits are derived from a combination of legislative action, judicial interpretations and federal requirements.

3. Schedule of Events

The following Schedule of Events represents ERSRI's best estimate of the schedule that will be followed.

RFP SCHEDULE OF EVENTS	
NOTICE: ERSRI reserves the right, at its sole discretion, to adjust this schedule as it deems necessary.	
EVENT	DATE
1. RFP Issued	August 1, 2018
2. Deadline for Vendor Questions	September 14, 2018
3. ERSRI Responds to Vendor Questions	September 21, 2018
4. Proposal Due	September 28, 2018
5. Interviews	Week of October 22, 2018
7. Contract Start Date	November 2018

Vendor questions are to be submitted via email to the RFP Administrator identified in Section 1. The questions shall constitute the bidders conference as defined in ERSRI Regulation No. 1.3, Rules Concerning the Selection of Consultants, Section 1.3.2(D)(3). Vendor proposals are to be submitted in accordance with the proposal preparation instructions provided in Section 6.

4. Project Scope

ERSRI is issuing this solicitation to perform an assessment of security controls on an ongoing basis to be conducted to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement of ERSRI's operations, internal controls and its current policies and procedures pertaining to its current IT environment. ERSRI is looking for a comprehensive and best practice Security Audit to include, but not limited to, the areas of concern below. Any additional materials and documentation can be referenced and attached with your submission.

The project's scope includes:

1. **Third Party On-Site Security Audit:** Assist ERSRI in performing a 3rd party security audit to confirm that security and data protection controls are in place and compliant to ERSRI's

business needs and in alignment with industry standards such as NIST 800-53 or other applicable industry acceptable standards. The Vendor used by ERSRI is Morneau Shepell located on Montreal and Toronto Canada.

- 2. Review existing IT Security Policies/Practices and Procedures** The vendor will review current state of Information security policies and standards and benchmark against ERSRI's business needs and commonly accepted industry standards such as ISO, NIST, OWASP and SANS to enhance the current policy set where there are gaps to the common standards, build new policies to match where existing controls are in place within ERSRI, and to make recommendations for additional policies that may be needed in order to become more closely aligned with the common standards and leading industry practices.

Deliverables -

- Review currently implemented information security policies and standards
 - Benchmark current policies and standards against ISO, NIST, OWASP and SANS standards
 - Review the discovered gaps and observations with ERSRI management
 - Develop and finalize revised information security policies and standards
- 3. Vulnerability Assessment** – Perform in-depth cybersecurity vulnerability assessment and penetration testing of ERSRI's logical and physical IT infrastructures:
- Internal Network - All internal corporate systems to include workstations, servers, switching/routing infrastructure, virtualization and storage infrastructure, and other connected IT devices. Including all Demilitarized (DMZ) systems to include flow controls from external to internal systems.
 - External Network - All external public facing systems to include firewalls, load balancers, web servers, ftp servers, and web service interface points.
 - Wireless Network – All wireless systems to include internal touch points from all SSID, broadcast or hidden, as well as encryption levels.
 - Physical access controls testing - Determine if the current physical security is effective by conducting physical access assessments;
 - Remote Access/External Partners – Assess remote access and security of network connections and data traffic to and from external partners
 - Social Engineering - perform social engineering procedures to verify the existence and effectiveness of procedural controls to prevent unauthorized physical and electronic access to ERSRI's and MS's IT systems. These procedures should be performed without the knowledge of Systems staff at a time to be coordinated with Executive Management
 - Internet usage – Asses URL/web filtering and access restrictions
 - Host based security – Assess security of critical systems at operating system and database layers and associated identity and access management controls.

Key Deliverables – The vendor will provide ERSRI with a detailed report on testing and attack scenarios used, vulnerabilities discovered, including the risk rating.

- Executive Summary with overall severity findings and risk exposure
 - Detailed technical results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots
 - Detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures
 - Remediation recommendations to close the deficiencies identified
 - Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies
- 4. Penetration Testing-** perform non-volatile exploit procedures designed to determine how well ERSRI's and MS's security systems can withstand up-to-date malicious exploits launched via dial-in, internet, and internal network connections.
- Testing will attempt to compromise networks and operating system to identify vulnerabilities to the system
 - Assess the provided network(s) to identify potential vulnerabilities.
 - Exploit vulnerabilities and provide evidence of unauthorized access to approved subnets and systems.
 - Penetration testing should be performed from two perspectives:
 - An outside with no approved system access.
 - A malicious insider who has access to the system.
 - Evidence gathered as proof of access must not harm the confidentiality, integrity, or availability of the systems, application, and or data.
 - Special attention should be given to areas that contain high risk data.

These procedures should be performed without the knowledge of ERSRI staff at a time to be coordinated with Executive Management.

If required and at the request of ERSRI, an additional scan shall be performed to assess whether vulnerabilities identified during initial scanning have been remediated satisfactorily.

- 5. Security Strategy and Systems** – evaluate ERSRI's and MS's security strategy and systems, including firewall hardware, software, placement and utilization. Perform an in-depth security scan and threat assessment to identify vulnerabilities. This should include, but not be limited to, port scans, host enumeration, and application/system identification.
- 6. Connections to External Partners** - review our connection and security posture to our external partners through wide area networks, dedicated circuits, ASP's, remote clients, and remote server technologies; Assess remote access and security of network connections and data traffic to and from external partners (External partners include, but is not limited to, ERSRI's custodian banks, system actuary and deposit banks.)
- 7. Inbound and Outbound Remote Access Strategy** – evaluate administration of remote access, both inbound and outbound. Review implications associated with the level of access that has been granted to authorized users including dial-up, Internet, Citrix for ASP connection

and staff access as well as MS user access protocol and procedures. Examine security issues in remote data transfer and the extent of network access available remotely. Perform a threat assessment to identify vulnerabilities with existing remote access.

- 8. Internet Usage** – evaluate how ERSRI secures sensitive data and applications: how we block unnecessary and unauthorized websites; and the tools we use for monitoring the URLs, links and Web pages that were visited. Identify any immediate problems. Assess URL/web filtering and access restrictions. Provide input on an action plan to handle potential on going or long-term problems.
- 9. Virus Protection** - evaluate the facility used to prevent impact from viruses. Perform a threat assessment to identify vulnerabilities.
- 10. Logon Security** - evaluate password and CRYPTO Card policies. Review current logon auditing practices. Examine current practices with regard to machine restrictions. Identify any potential weaknesses. Provide input on an action plan to deal with problems. Perform a threat assessment to identify vulnerabilities.
- 11. Fraud and General Controls Objectives:** Assess the risk that a single trusted user, administrator or vendor of ERSRI's or MS's Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in MS's information systems. Special attention should be given to:
 - segregation of duties,
 - documented and applied policies and procedures,
 - acquisition, development and change control practices,
 - database administration practices,
 - production control practices,
 - access and transaction authorizations,
 - monitoring practices, and
 - disaster recovery and incident response.
- 12. Member Service Systems Control Vulnerabilities-** assess the risk that a single trusted user, administrator or vendor of ERSRI's or MS's Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in ERSRI's member service systems.
- 13. Employer reporting Service Systems Control Vulnerabilities** - assess the risk that a single trusted user, administrator or vendor of ERSRI's or MS's Information Systems can accomplish and/or conceal the improper diversion of assets using vulnerabilities found in ERSRI's employer reporting service systems
- 14. Accounting and Administrative Systems Control Vulnerabilities-** assess the risk that a single trusted user, administrator or vendor of ERSRI's or MS's (Crowe Horwath is MS's subcontractor and implementor of the accounting system) Information Systems can

accomplish and/or conceal the improper diversion of assets using vulnerabilities found in ERSRI's accounting and administrative systems.

- 15. Develop a Vulnerability Assessment Plan:** The vendor will conduct a comprehensive Cybersecurity Program maturity assessment using an objective and independent framework developed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) including ERSRI's people, organizational structure, processes and supporting technology.

The overall objectives of this phase will be to assist ERSRI in gaining an understanding of the existing maturity of the Cybersecurity program in comparison to industry standards, develop a sustainable risk management program, and provide observations and recommendations for overall program improvement.

Key Tasks – Assess ERSRI's ability to protect its information assets and its preparedness against cyber-attack on the following items:

- Leadership and governance: Board and Management, their due diligence, ownership, and effective management of risk within the context of the organization's goals, objectives and the external threat/risk landscape.
- Human factors: The level of security-focused culture that empowers and ensures the right people, skills, culture and knowledge.
- Information risk management: Organization's approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.
- Operations and technology: The level of control measures implemented within organization to address identified risks, and minimize the impact of compromise.
- Business continuity: Organizations preparations for a security incident and its ability to prevent or minimize the impact through successful crisis and stakeholder management.
- Legal and compliance: Legal and regulatory compliance requirements relevant to the organization.

Deliverables:

- Maturity and risk rating based on NIST CSF, including but not limited to:
 - Highlight successes and identify gaps based on CSF target maturity of "Implemented" or level 3
 - Security maturity comparison against similar organizations (public sector) and similarly sized organizations
 - Rank criticality of gaps
- Identify security/privacy risks in current practices inclusive of:
 - Organizational/Personnel (Skill/Knowledge Level)
 - Policy/Process/Procedures
 - Tools, Methods, Implementation and Operations specific issues
 - Access, implementation of NIST, industry/leading practices

- Dependencies between ERSRI and other state agencies as well as IT infrastructure service providers
- Develop detailed recommendations to close gaps which includes:
 - Recommend mitigation solutions
 - Estimated budget requirements range for mitigation deployment and ongoing support
 - Staffing requirements range for both deployment and ongoing support
 - Estimated deployment timelines

The vendor shall propose a recommended ongoing risk management and vulnerability review in which the vendor will be on-site at the ERSRI offices managing the vulnerability assessment plan developed by them and approved by ERSRI. The term of such on-site review shall begin after item #16 "Prepare a final report" has been delivered and approved by ERSRI for an initial period of three (3) years. The vendor should provide cost options to extend the initial period for an additional 3 years.

16. Prepare a final report: Develop a report with the vendor's assessment of the ERSRI's, MS's and its subcontractor's IT risk management policies, practices, and procedures and present the findings to executive management with a prioritized list of recommended or required improvements. The final report should contain an executive summary and presentation suitable for non-technical management.

17. Provide a comprehensive Security Training to all Staff: Upon completion of the assessment, the vendor should provide a comprehensive training/presentation to all ERSRI staff outlining best practices for security awareness. Online testing of employee comprehension of security awareness would be required for the vendor to provide.

5. Vendor Preferences

Preference will be given to vendors who can offer the services of a Security Analyst with at least 5 years' experience with security technologies, including planning, architecture, policies and procedures. This Analyst should possess one or more of the following certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), or Certified Computer Examiner.

Preference will be given to vendors who can offer the services of a Project Manager to oversee the engagement with at least 5 years of project management experience. This Project Manager should possess either a CAPM or PMP certification and ideally have demonstrable work history with technology audits and assessments.

Preference will also be given to vendors who are **Certified in Risk and Information Systems Control (CRISC)** certification.

- The Firm should indicate, if any, experience in providing these services to state and municipal agencies or public/private retirement systems.

6. Proposal Preparation

Each response to this RFP must consist of a Technical Proposal and a Cost Proposal (as described below).

Each Vendor must submit an original signed Technical Proposal to ERSRI in a sealed package that is clearly marked "*Technical Proposal in Response to RFP No. 2018-001*". The Vendor must then email copies of the Technical Proposal titled "*Technical Proposal in Response to RFP No. 2018-001*" that includes the technical proposal in Microsoft Word format as submitted in hardcopy, and another containing the technical proposal in PDF format with confidential information redacted or removed to frank.karpinski@ersri.org.

Each Vendor must submit its original signed Cost Proposal in a separate sealed package that is clearly marked "*Cost Proposal in Response to RFP No. 2018-001*". The Vendor must then email copies of the Cost Proposal titled "*Cost Proposal in Response to RFP No. 2018-001*" that includes the cost proposal as submitted in Microsoft Word and/or Excel format, and the cost proposal in PDF format to frank.karpinski@ersri.org.

If the Vendor encloses the separately sealed proposals (as detailed above) in a larger package for mailing, the Vendor must clearly mark the outermost package:

Contains Separately Sealed Technical and Cost Proposals for RFP No. 2018-001

ERSRI must receive all proposals in response to this RFP at the address specified in Section 1 no later than the deadline stipulated in Section 3, Schedule of Events.

A Vendor may not deliver a proposal orally.

It is the Vendor's responsibility to ensure that ERSRI receives the proposal.

NOTICE: No pricing information shall be included in the Technical Proposal. Inclusion of such information in the Technical Proposal shall render the full proposal disqualified from consideration.

6.1 Technical Proposal

Each proposal should be economically prepared, with emphasis on completeness and clarity of content. A proposal, as well as any reference material presented, must be written in English and printed in single-column format on standard 8 1/2" x 11" paper (although foldouts containing charts, spreadsheets, and oversize exhibits are permissible). All proposal pages must be numbered.

The Technical Proposal must include:

- **Title Page** bearing the RFP number and project title, as well as Vendor name, address, and contact information.
- **Table of Contents**
- **Vendor Information**

Identification of the Vendor's form of business (whether individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and prime liaison (name, mailing address and telephone number) who ERSRI may contact regarding the proposal.

Number of years Vendor has been in business, as well as the number of years vendor has performed the services specifically required by this RFP.

Statement of Vendor's intent to use subcontractors, and if so, the names and mailing addresses of committed subcontractors as well as a description of the scope and portions of the work each subcontractor will perform.

Disclosure of whether the Vendor has undergone within the past ten (10) years any mergers, acquisitions, sales or significant changes in partnership interests, and if so, an explanation providing relevant details. Include in this statement the likelihood of any mergers, acquisitions, sales or significant changes in partnership interests in the next three (3) years.

A statement of whether the Vendor or any of the Vendor's employees, agents, independent contractors, and/or subcontractors have been convicted of, pleaded guilty to, and/or pleaded *nolo contendere* to any felony, and if so, an explanation providing relevant details.

A statement of whether there is any pending litigation against the Vendor, and if such litigation exists, an attached opinion of counsel as to whether the pending litigation will impair the Vendor's performance in a contract under this RFP.

Provide a statement of whether the Vendor has filed (or had filed against it) within the past ten (10) years any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors, and if so, an explanation providing relevant details.

Provide a statement as to whether any of the Vendor's previous contracts with public retirement system clients were terminated prior to the expiration of the contract term, and if so, provide an explanation of the circumstances.

Provide a statement as to whether the Vendor or any of its officers, directors, and/or staff members proposed by the Vendor to perform work for ERSRI have any possible conflict of interest.

Please indicate whether your company conducts a Bureau of Criminal Identification (BCI) check and if so, provide documentation that these BCI checks were administered including the results of the reports for the staff who will be involved in the risk assessment project. Otherwise, a BCI check is required for all members of staff who will be part of the assessment.

- **Vendor Qualifications and Experience**

Details of the Vendor's credentials to perform the services being sought by ERSRI in the public retirement systems industry.

Provide information on the Vendor's history of providing the requested services. Address Vendor's experience in providing security risk technology evaluation and implementation strategies, and Vendor methodologies and tools that will be used to expedite the delivery of the requested services.

Information about the Vendor's proposed engagement team, to include detailed resumes of all proposed staff, a project organization chart, and rationale behind particular assignments of roles and responsibilities. Also, corresponding information on any subcontractors that will participate in the project.

A list of at least three (3) references from public retirement systems, state agencies, municipalities, not-for-profit organizations and publicly traded or privately held corporations willing to discuss with ERSRI the Vendor's performance in providing services comparable to the services being sought by ERSRI. Each reference must include the agency name and address; the name, title, and phone number of the contact person at the agency/company; the time period during which the services were provided; the name of the Vendor's lead project manager on the engagement; and a brief summary of the services provided.

- **Technical Approach**

Details of Vendor's proposed technical approach to each of the project scope elements discussed in Section 4, Project Scope.

A narrative illustrating how the Vendor will manage the project, ensure completion of the scope of services, and accomplish ERSRI's objectives.

A high-level Gantt chart of proposed project activities illustrating the expected timing of the engagements deliverables.

- **Proposed Contract**

A copy of the contract for services that the Vendor anticipates executing should ERSRI select the Vendor.

The Technical Proposal shall be incorporated into the contract by reference.

6.2 Cost Proposal

The cost proposal should detail projected expenditures of time and material *not to be exceeded*. The cost schedule must include the hours to be expended on each of the seventeen (17) tasks identified in Section 4, Project Scope; the hourly rate applicable to each Vendor staff category; total projected expenditures for each task; and a projected grand total. Please include an estimate of the travel-related expenses anticipated by the Vendor, to include review of MS and other external partners. Expenses may be expressed either as a percentage of service costs or as part of the Vendor's hourly rates. Travel related expenses must *be included in the not-to-exceed project cost*.

Vendors should provide an optional cost proposal to allow ERSRI to perform a second audit and their recommendation of when such an audit should be performed again.

The finalized negotiated Cost Proposal shall be incorporated into the contract by reference.

7. Proposal Evaluation and Contract Award

Vendor selection and contract award will be at the sole discretion of ERSRI. Vendor proposals will be evaluated on the basis of the following criteria:

CRITERION	% WEIGHT
Qualifications of the Firm	30%
Proposed Staff Qualifications & Project Organization	20%
Audit Plan & Approach	20%
Completeness of Responses	10%
Vendor References	10%
Cost	10%
Total	100%

ERSRI reserves the right to make no award.

8. Procurement and Contract Administration

Contract Term

Period of performance will be determined during contract negotiations prior to award. If options are selected, it is anticipated that this project may span more than one State fiscal year (July 1-June 30) and/or multiple calendar years.

At the termination of the contract by either conclusion or mutual cancelation, the vendor MUST return any ERSRI data maintained by them or legally certify that it has destroyed such data.

Required Review

Bidders shall carefully review this solicitation for defects and questionable or objectionable matter. Comments concerning defects and questionable or objectionable material must be made in writing and received by the RFP Administrator at least fifteen (15) days prior to proposal opening to allow for the issuance of any necessary amendments.

Questions Received Prior to Opening of Proposals

All questions must be directed to the issuing office, addressed to the RFP Administrator. Bidders are required to put questions in writing; questions must be received no later than the date stipulated in Section 3, Schedule of Events.

Responses to all questions will be provided to all vendors who have submitted bids. Questions and answers will be incorporated by reference into the ensuing awarded contract as appropriate.

Should the issuing office consider it necessary to revise any part of this RFP, addenda will be provided to all bidders who have been provided the RFP.

Cancellation

ERSRI may cancel an invitation for bids, a request for proposal, or negotiations in connection with the procurement of any item or service or may reject all bids or proposals if ERSRI determines that such action is in its best interest. No such cancellation or rejection shall prevent ERSRI from re-soliciting supplies and services for the same project on the same or different terms.

Confidentiality of Proposal Information

ERSRI shall treat all documents submitted by a Vendor in response to this RFP as public records upon the selection of a firm. The release of public records is governed by Rhode Island General Laws §38-2-1 et seq. ("APRA"). Vendors are encouraged to familiarize themselves with this law before submitting a proposal.

By submitting a proposal, Vendors agrees that ERSRI may reproduce Vendor's proposal for purposes of facilitating the evaluation of the proposal or to respond to requests for public records. Vendor consents to such reproduction by submitting a proposal and further warrants that such reproduction does not violate its rights or the rights of any third parties.

Any request by a Vendor that records submitted by them be exempt from being considered public record must be included in the cover letter with the Vendor's proposal. In addition, the Vendor must enumerate the specific grounds upon which the APRA or other applicable law supports treatment of the documents as exempt from being considered a public record, and further, the factual basis, if any, upon which they rely in asserting that the documents should be exempt. Any request for treating records submitted as being exempt must also include: the name, address, and telephone number of the person authorized by the Vendor to respond to any inquiries by the ERSRI regarding such an assertion.

Any proposals submitted which contain non-public records must be conspicuously marked on the outside as containing non-public information, and each page upon which non-public information appears must be conspicuously marked as containing non-public information. Identification of the entire proposal as being non-public records may be deemed non-responsive and may disqualify the Vendor.

If the Vendor designates any portion of the proposal as being a non-public record, the Vendor must submit one (1) copy of the proposal from which the non-public record is deleted or redacted. This copy shall be submitted in addition to the number of copies requested in this RFP. The non-public records must be excised in such a way as to allow the public to determine the general nature of the information redacted and retain as much of the proposal as possible.

ERSRI will treat the records marked as non-public as being confidential information to the extent such information is determined confidential under the APRA or other applicable law or by a court of competent jurisdiction. The Vendor's failure to request records submitted as being non-public records will be deemed as a waiver of any right to confidentiality, which the Vendor may have had.

All proposals and other material submitted become the property of ERSRI and will not be returned. ERSRI reserves the right to use any ideas presented in any response to the RFP.

Bid Preparation Costs

No costs incurred by the bidder in preparation of its proposal, including travel and personal expenses, may be charged as an expense of performing the contract.

ERSRI shall not pay for costs incurred for proposal or contract preparation as a result of termination of this RFP or termination of the contract resulting from this RFP.

Single Source of Support

The successful contractor shall be granted the right to subcontract a portion of the work but shall retain sole responsibility for the successful delivery of all contracted deliverables. The prime contractor must be designated in the proposal, and any use of subcontractors must be clearly explained. All references in this RFP to the contractor, vendor, or successful bidder shall be construed to encompass both the prime contractor and all subcontractors and infer the single source of support from the prime contractor.

If the use of subcontractors is planned, the proposal must specifically identify the tasks that each subcontractor is to perform. All subcontractor staff in key positions must meet the same qualifications for experience specified for the prime contractor. Resumes should be included for these key subcontractor staff. The proposal must also include sample copies of any agreements to be executed between the prime contractor and any subcontractors in the event of contract award. All subcontracting agreements must be signed at the time of contract award, and executed copies provided to ERSRI for review prior to the execution of a contract with the prime contractor.

All bidders must list in their proposal the complete names and addresses of the subcontractors, and the type and percentage of work they will be providing and must include a signed, written statement from any proposed subcontractors verifying their commitment to perform the services indicated to be completed by them.

Substitution of any proposed subcontractor is only allowed following written permission from the RFP Administrator.

Joint ventures shall not be acceptable for the performance of this contract.

Bidder's Certification

By signature on their proposal, each bidder certifies that they are complying with or will comply with:

1. the laws of the State of Rhode Island;
2. the applicable portion of the Federal Civil Rights Act of 1964;
3. Equal Employment Opportunity federal executive order 11246, as amended, and Section 28-5.1-10 of the General Laws of the State; and
4. all terms and conditions delineated in this RFP.

Additionally, in signing their proposal, each bidder guarantees that the price submitted was calculated independently and without collusion.

If any bidder fails to comply with items 1 through 4 of the above paragraph, ERSRI reserves the right to disregard the proposal, terminate the contract, and/or consider the contractor in default.

News Releases

News releases pertaining to this RFP or the project to which it relates shall not be made without prior approval of the Executive Director, and then only in coordination with ERSRI. Failure to adhere to this procedure is grounds for termination of the contract.

Annual Appropriations

All contracts awarded by ERSRI shall be subject to the available funds of budgets approved by the ERSRI Retirement Board and the General Assembly.

Notice of Intent to Award

ERSRI may conduct written or oral discussions with responsible bidders who submit proposals that ERSRI determines in writing to be reasonably likely for selection. Discussions shall not disclose any information derived from proposals submitted by competing bidders. Discussions need not be conducted:

1. with respect to prices, where such prices are fixed by law or regulation, except that consideration shall be given to competitive terms and conditions; or
2. where time of delivery or performance will not permit discussions; or
3. where it can be clearly demonstrated and documented from the existence of adequate competition or accurate prior cost experience with the particular hardware, software, or service item, that acceptance of an initial offer without discussion would result in fair and reasonable prices, and the request for proposals notifies all bidders of the possibility that award may be made on the basis of the initial offers.

Oral Presentations

ERSRI may at its discretion require bidders to make an oral presentation of their proposals on-site at ERSRI offices. Participants on ERSRI's behalf may include up to ten (10) people. Bidder participants should include at least one person but no more than five (5) persons who are knowledgeable of the RFP and the response submitted by the bidder's organization, and who are qualified to answer questions relating to the proposal.

Oral presentations, if conducted, will not involve with bidders' cost proposals. Cost negotiations, if and when appropriate, will be conducted separately.

The purpose of the oral presentations, if conducted, will be to:

- provide a summary of the respective bidder's proposal for the benefit of ERSRI, senior management and/or board members; and
- permit ERSRI and staff to ask questions pertaining to the bidder's proposal.

Bidders will be provided no more than one half hour each for their oral presentations, to be inclusive of a summary of the proposal contents and a question-and-answer session with ERSRI staff. Each bidder will be offered three (3) alternative dates for scheduling the oral presentation. Oral presentations may be recorded at the discretion of ERSRI. Bidder attendance at the oral presentations should include the proposed on-site manager.

Restrictions on Gifts

State ethics laws restrict gifts which may be given or received by employees and directors and requires certain individuals to disclose information concerning their activities with State government. Vendors are responsible to determine the applicability of these laws to their activities and to comply with the requirements. In addition, it is a felony offense to bribe or attempt to bribe a public official.

State Code of Ethics

ERSRI is committed to maintaining the highest standards of ethics in the awarding of contracts. Vendors should be familiar with and abide by the State Code of Ethics, as set forth in Rhode Island General Laws §36-14-1 *et. seq.* and any additional regulations as provided on the State Ethic's Commission website: <http://www.ethics.ri.gov/code/>.

Non-Discrimination

All proposals shall be considered based on their merit in accordance with the criteria specified herein and shall not exclude any person, firm, or other entity, from consideration on the grounds of race, color, religion, sex, sexual orientation, gender identity or expression, age, national origin, disability, or veteran status. For more information, see the State of Rhode Island Office of Diversity, Equity & Opportunity website at <http://odeo.ri.gov/offices/eoo/>. Further, see the Treasury's Equal Opportunity Report for 2016 at <http://data.treasury.ri.gov/dataset/eeop-utilization-report>.

Limitation of Liability

The failure of the vendor or any of its subcontractors to employ commercially reasonable measures in accordance with industry standards to protect against unauthorized access, use or disclosure of ERSRI pension plan member data held directly by the Vendor or such subcontractor (as the case may be), there shall be no limitation of liability.

**Employees' Retirement System of the
State of Rhode Island
And
Municipal Employees' Retirement System
of the State of Rhode Island**

Regulation No. 1.3

Rules Concerning the Selection of Consultants

1.3 Rules Concerning the Selection of Consultants

1.3.1 General Provisions

A. Introduction.

1. The Employees' Retirement System of the State of Rhode Island and the Municipal Employees' Retirement System of the State of Rhode Island (the "System") are authorized to employ consulting and other professional services. The purpose of these rules is to adopt internal procedures consistent with the requirements of Chapter 2 of Title 37 of the Rhode Island General Laws (State Purchases Act) in connection with the procurement of consulting services by the System.

B. Definitions.

1. All capitalized terms used herein shall have the same meaning as set forth in the "Rules of the Employees' Retirement System of the State of Rhode Island and the Municipal Employees' Retirement System of the State of Rhode Island for the Procurement of Supplies and Services". The words defined in this subsection shall have the following meanings wherever they appear in these Rules, unless the context in which they are used clearly requires a different meaning.
 - a. "Consultant" shall mean any person engaged to provide information regarding a particular area of knowledge in which the person has expertise, including, but not limited to, accountants, actuaries, financial consultants, data processing consultants and physicians, excluding, however, legal services.

C. Application of Rules.

1. These Rules apply to all expenditures of funds by the System under a contract for consulting services, except contracts between the System and the State of its political subdivisions, or between the System and other governments. The provisions of these Rules shall be considered to be incorporated in all contracts of the System to which they apply.
2. Notwithstanding anything contained in this Section 1.3.1(C), the "Rules of the Employees' Retirement System of the State of Rhode Island and the Municipal Employees' Retirement System of the State of Rhode Island for the Procurement of Supplies and Services" shall govern the procurement of supplies and services.

D. Procurement Responsibilities of the System.

1. The Procurement Committee shall select persons or firms to render consultant services pursuant to these Rules. Accordingly, the term "System" shall be used in these Rules to designate the Procurement Committee.

E. Public Access to Procurement Records.

1. Except as otherwise provided for herein all procurement records of the System shall be public record to the extent provided in Chapter 2 of Title 38 (Access to Public Records) of the General laws of Rhode Island and shall be available to the public as provided in such Act.

F. Procurement Decisions of the System.

1. Every determination required by these Rules shall be in writing and based upon written findings of fact by the System. These determinations and written findings shall be retained in an official contract file in the offices of the System.

1.3.2 Selection of Consultants

A. General Policy.

1. It shall be the policy of the System to publicly announce its requirements for consulting services, which are reasonably estimated to exceed ten thousand dollars (\$10,000), and to negotiate contracts for such professional services on the basis of demonstrated competence and qualifications and at fair and reasonable prices.

B. Annual Statement of Qualifications and Performance Data.

1. Consultants shall be encouraged by the Executive Director to submit to the System annually a statement of qualifications and performance data which shall include, but not be limited to the following:
 - a. The name of the firm and the location of its principal place of business and all offices;
 - b. The age of the firm and its average number of employees over the past five years;
 - c. The education, training, and qualifications of members of the firm and key employees;

- d. The experience of the firm, reflecting technical capabilities and project experience; and
 - e. Such other pertinent information as requested by the Executive Director.
- C. **Public Announcement of Needed Consultant Services.**
 1. The System shall give public notice in a newspaper of general circulation in the State of the need for consultant services which are reasonably estimated to exceed ten thousand dollars (\$10,000). The System may publish such additional notice as it deems necessary to assure response from qualified individuals or firms. Such public notice shall be published sufficiently in advance of the date when responses must be received in order that interested parties have an adequate opportunity to submit a statement of qualifications and performance data. The notice shall contain a brief statement of the services required, describe the project and specify how a solicitation containing specific information on the project may be obtained.
- D. **Solicitation.**
 1. A solicitation shall be prepared which describes the System's requirements and sets forth the evaluation criteria. It shall be distributed to interested persons.
 2. The solicitation shall describe the criteria to be used in evaluating the statement of qualification and performance data and in the selection of firms. Criteria shall include, but are not limited to:
 - a. competence to perform the services as reflected by
 - b. technical training and education; general experience; experience in providing the required services; and the qualifications and competence of persons who would be assigned to perform the services;
 - c. ability to perform the services as reflected by workload
 - d. and the availability of adequate personnel, equipment, and facilities to perform the services expeditiously;
 - e. past performance as reflected by the evaluation of private persons and officials of other governmental entities that have retained the services of the firm with respect to such factors as control of costs, quality of work, and ability to meet deadlines; and the cost of such services.

3. For services reasonably estimated to exceed twenty thousand dollars (\$20,000), a bidder's conference shall be held which describes the criteria to be used in evaluating the statement of qualification and performance data and in the selection of firms. The scope of work shall be discussed and further defined at such conference, including on-site visits, if appropriate.

E. Evaluation of Statements of Qualifications and Performance Data.

1. The consultant selection committee shall evaluate statements that may be submitted in response to the solicitation of consultant services and statements of qualifications and performance data, if required. All such statements shall be evaluated in light of the criteria set forth in the solicitation for consulting services. The consultant selection committee may waive informalities in any such statements.

F. Final Selection of Contractors.

1. The consultant selection committee shall select no more than three (3) firms (or two (2) if only two (2) apply) evaluated as being professionally and technically qualified. The firms selected, if still interested in providing the services, shall make a representative available to the consultant selection committee at such time and place as it shall determine, to provide such further information as it may require.
2. The consultant selection committee shall negotiate with the highest qualified firm for a contract for consulting services for the System at compensation which the consultant selection committee determines to be fair and reasonable. In making such determination, the consultant selection committee shall take into account the professional competence and technical merits of the offerors, and the price for which the services are to be rendered. The consultant selection committee shall be responsible for the final selection of the providers of consulting services.

G. Contracts Not Exceeding \$10,000.

1. The Executive Director of the System shall be responsible for the final decision on consulting contracts not expected to exceed ten thousand dollars (\$10,000). The Executive Director shall, however, notify the Department of Administration, the Division of Purchases and the Division of Budget of the State of its selection. The Executive Director shall use the criteria set forth in Section 1.3.2(D)(2) in making such determinations. Each determination shall be justified in writing.

1.3.3 Remedies

A. Protest of Solicitation and Award.

1. Any actual or prospective contractor who is aggrieved in connection with the solicitation or award of any contract under these Rules may file a protest with the System. A protest must be filed in writing not later than two (2) calendar weeks after such aggrieved person knows or should have known of the facts giving rise thereto.
2. The System shall promptly issue a decision in writing regarding such protest. A copy of that decision shall be furnished to the aggrieved party and shall state the reasons for the action taken.
3. In the event a protest is filed in a timely manner under this Section, the System shall not proceed further with the solicitation or award which is the subject of the protest until it has issued a decision on the protest, or determined that continuation of the procurement is necessary to protect a substantial interest of the System.

B. Debarment and Suspension.

1. After reasonable notice to the person involved and reasonable opportunity for that person to be heard, the System may debar a person for cause from consideration for award of contracts contemplated by these Rules. The debarment shall not be for a period of more than three years. The System may suspend a person from consideration for award of contracts if there is probable cause for debarment. The suspension shall be for a period of not less than three months.
2. The causes for debarment or suspension include the following:
 - a. conviction of a criminal offense in connection with obtaining or attempting to obtain a public or private contract or subcontract, or in the performance of such contract or subcontract;
 - b. conviction under state or federal statutes of embezzlement, theft, forgery, bribery, falsification or destruction of records, stolen property, or any other offense indicating a lack of business integrity or business honesty which currently, seriously, and directly affects responsibility as a contractor with the System;
 - c. conviction under state or federal antitrust statutes arising out of the submission of bids or proposals;

- d. violation of contract provisions, as set forth below, of a character which is regarded by the System to be so serious as to justify debarment action, including,
 - (1) deliberate failure without good cause to perform in accordance with the specifications or within the time limit provided in the contract; or
 - (2) a recent record of failure to perform or of unsatisfactory performance in accordance with the terms of one or more contracts; provided that failure to perform or unsatisfactory performance caused by acts beyond the control of the contractor shall not be considered to be a basis for debarment;
- e. any other cause the System determines to be so serious and compelling as to affect responsibility as a contractor, including debarment by a governmental entity.

- 3. The System shall issue a written decision to debar or suspend. The decision shall state the reasons for the action taken; and inform the debarred or suspended person of its rights to judicial review.
- 4. A copy of the decision under Subsection (3) of this Section shall be furnished promptly to the debarred or suspended person.

C. Resolution of Contract Disputes.

- 1. If any claim or controversy arising under contracts to which these Rules apply is not resolved by mutual agreement, the System shall promptly issue a decision in writing regarding the subject matter of such claim or controversy. A copy of that decision shall be furnished to the contractor. If the System does not issue a written decision within thirty (30) days after written request for a final decision, or within such longer period as might be established by the parties to the contract in writing, then the contractor may proceed as if an adverse decision had been received from the System.

1.3.4 Additional Matters

A. Equal Employment Opportunity.

- 1. For all contracts for consultant services exceeding ten thousand dollars (\$10,000), contractors must comply with the requirements of federal executive order 11246, as amended, and Section 28-5.1-10 of the General Laws. Failure to comply will be considered a substantial breach of the contract subject to

penalties prescribed in regulations administered by the Department of Administration of the State.

B. Conflict of Interest.

1. No member or employee of the System shall have any interest, financial or otherwise, direct or indirect, or engage in any activity which is in substantial conflict with the proper discharge of his or her duties as a member or employee of the System.

1.3.5 Effective Date

A. Effective Date.

1. These Rules shall become effective upon adoption by the Board. Thereafter, the Board shall file a copy of these Rules with the Secretary of State.

B. Contracts in Effect on Effective Date.

1. These Rules shall not change in any way a contract commitment by the System or of a contractor to the System which was in existence on the effective date of these Rules.