


|   |   |  |  |
|---|---|--|--|
|  | <p><b>State of South Carolina</b></p> <p><b>South Carolina Public Employee Benefit Authority</b></p> <p><b>Request for Proposal Amendment 1</b></p> | <p>Solicitation Number: PEBA0412023<br/> Date Issued: <b>01/22/2024</b><br/> Procurement Officer: Georgia Gillens, CPPO, CPPB, NIGP-CPP<br/> Phone: 803.734.0010<br/> E-mail Address: <a href="mailto:GGillens@peba.sc.gov">GGillens@peba.sc.gov</a></p> |  |
|---|---|--|--|

**DESCRIPTION: Provide Group Vision Benefits Plan for the S.C. Public Employee Benefit Authority**

**SUBMIT OFFER BY (Opening Date/Time): February 7, 2024 12:00 P.M.**

*The Term "Offer" Means Your "Proposal". Your offer must be submitted in a sealed package. The Solicitation Number & Opening Date should appear on the package exterior. See the clause entitled "Submitting Your Offer or Modification."*

**SUBMIT YOUR SEALED OFFER TO EITHER OF THE FOLLOWING ADDRESSES:**

|   |   |
|---|---|
| <p><b>MAILING ADDRESS:</b><br/> South Carolina Public Employee Benefit Authority<br/> P.O. Box 11960<br/> Columbia, S.C. 29211-1960<br/> Attention: Georgia Gillens, CPPO, CPPB</p> | <p><b>PHYSICAL ADDRESS:</b><br/> South Carolina Public Employee Benefit Authority<br/> 202 Arbor Lake Drive<br/> Columbia, S.C. 29223<br/> Attention: Georgia Gillens, CPPO, CPPB</p> |
|---|---|

|                                      |   |
|--------------------------------------|---|
| <p><b>AWARD &amp; AMENDMENTS</b></p> | <p>Award will be posted on <b>March 7, 2024</b>. The award, this solicitation, any amendments, and any related notices will be posted at the following web address: <a href="https://procurement.sc.gov/vendor/contracts/other-solicitations/peba">https://procurement.sc.gov/vendor/contracts/other-solicitations/peba</a></p> |
|--------------------------------------|---|

You must submit a signed copy of this form with Your Offer. By submitting a proposal, You agree to be bound by the terms of the Solicitation. You agree to hold Your Offer open for a minimum of one hundred twenty (120) calendar days after the Opening Date. (See the clause entitled "Signing Your Offer.")

|   |   |  |
|---|---|--|
| <p><b>NAME OF OFFEROR</b><br/><br/> <small>(Full legal name of business submitting the offer)</small></p>   | <p>Any award issued will be issued to, and the contract will be formed with, the entity identified as the Offeror. The entity named as the offeror must be a single and distinct legal entity. Do not use the name of a branch office or a division of a larger entity if the branch or division is not a separate legal entity, i.e., a separate corporation, partnership, sole proprietorship, etc.</p> |  |
| <p><b>AUTHORIZED SIGNATURE</b><br/><br/> <small>(Person must be authorized to submit binding offer to contract on behalf of Offeror.)</small></p> |   |  |
| <p><b>TITLE</b><br/><br/> <small>(Business title of person signing above)</small></p>   | <p><b>STATE VENDOR NO.</b><br/><br/> <small>(Register to obtain S.C. Vendor No. at <a href="http://www.procurement.sc.gov">www.procurement.sc.gov</a>)</small></p>  |  |
| <p><b>PRINTED NAME</b><br/><br/> <small>(Printed name of person signing above)</small></p>  | <p><b>DATE SIGNED</b></p>   | <p><b>STATE OF INCORPORATION</b><br/><br/> <small>(If you are a corporation, identify the state of incorporation.)</small></p> |

**OFFEROR'S TYPE OF ENTITY: (Check one)** (See "Signing Your Offer" provision.)

Sole Proprietorship  Partnership  Other \_\_\_\_\_

Corporate entity (not tax-exempt)  Corporation (tax-exempt)  Government entity (federal, state, or local)

**PAGE TWO**  
**(Return Page Two with Your Offer)**

|  |  |
|--|--|
| <b>HOME OFFICE ADDRESS</b> (Address for offeror's home office / principal place of business) | <b>NOTICE ADDRESS</b> (Address to which all procurement and contract related notices should be sent.)<br><br>_____ Area Code -<br>Number - Extension Facsimile<br>_____<br>E-mail Address<br>_____ |
|--|--|

|   |   |
|---|---|
| <b>PAYMENT ADDRESS</b> (Address to which payments will be sent.)<br><br>_____ Payment Address same as Home Office Address<br>_____ Payment Address same as Notice Address ( <b>check only one</b> ) | <b>ORDER ADDRESS</b> (Address to which purchase orders will be sent)<br><br>_____ Order Address same as Home Office Address<br>_____ Order Address same as Notice Address ( <b>check only one</b> ) |
|---|---|

**ACKNOWLEDGMENT OF AMENDMENTS**  
 Offerors acknowledges receipt of amendments by indicating amendment number and its date of issue. (See the clause entitled "Amendments to Solicitation")

| Amendment No. | Amendment Issue Date | Amendment No. | Amendment Issue Date | Amendment No. | Amendment Issue Date | Amendment No. | Amendment Issue Date |
|---------------|----------------------|---------------|----------------------|---------------|----------------------|---------------|----------------------|
|               |                      |               |                      |               |                      |               |                      |
|               |                      |               |                      |               |                      |               |                      |

|   |                      |                      |                      |                         |
|---|----------------------|----------------------|----------------------|-------------------------|
| <b>DISCOUNT FOR PROMPT PAYMENT</b><br>(See the clause entitled "Discount for Prompt Payment") | 10 Calendar Days (%) | 20 Calendar Days (%) | 30 Calendar Days (%) | _____ Calendar Days (%) |
|---|----------------------|----------------------|----------------------|-------------------------|

|  |
|--|
|  |
|--|

## REQUEST FOR PROPOSAL – PEBA0412023

### Provide Group Vision Benefits Plan for the S.C. Public Employee Benefit Authority

**PLEASE NOTE:** The original Request for Proposal document stands as written with the exception of dates, the Schedule of Key Dates and Clause 7.40. Amendment 1 is being issued to answer questions submitted in writing by the deadline. See Attachment 17 -- Questions and Answers for your information. Any changes agreed to as a result of Attachment 17, Q&A have been listed below. The questions and answers submitted in writing by the deadline are included as an attachment for information only. Only the changes incorporated in Amendment 1 are relevant.

**Page 7, Replace Schedule of Key Dates in the Procurement Process with the following:**

#### SCHEDULE OF KEY DATES IN THE PROPOSAL PROCESS

All dates subject to change

|   |            |
|---|------------|
| 1. Distribution of the Request for Proposal                                     | 12/18/2023 |
| 2. Questions on the Request for Proposal  | 01/05/2024 |
| 3. Pre-proposal Conference and Final Deadline for Submission of all Questions.  | 01/17/2024 |
| 4. PEBA's Written Responses to Questions Submitted/Amendment Issued (tentative) | 01/22/2024 |
| 5. Submission and Opening of Proposals (12:00 p.m. E.T.)                        | 02/07/2024 |
| 6. Intent to Award Posting Date   | 03/07/2024 |
| 7. Intent to Award Becomes Official (tentative)                                 | 03/19/2024 |
| 8. Contract Performance   | 01/01/2025 |

See pages 47-49 Clause 7.40 INFORMATION SECURITY - SAFEGUARDING REQUIREMENTS (FEB 2015)

#### 7.40 INFORMATION SECURITY - SAFEGUARDING REQUIREMENTS (FEB 2015)

(a) *Definitions.* The terms used in this clause shall have the same meaning as the terms defined in the clause titled Information Security – Definitions. In addition, as used in this clause—

**Clearing** means removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

**Intrusion** means an unauthorized act of bypassing the security mechanisms of a system.

**Media** means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, large scale integration memory chips, and printouts (but not including display media, e.g., a

computer monitor, cathode ray tube (CRT) or other (transient) visual output) onto which information is recorded, stored, or printed within an information system.

**Safeguarding** means measures or controls that are prescribed to protect information.

**Voice** means all oral information regardless of transmission protocol.

(b) *Safeguarding Information.* Without limiting any other legal or contractual obligations, Contractor shall implement and maintain reasonable and appropriate administrative, physical, and technical safeguards (including without limitation written policies and procedures) for protection of the security, confidentiality and integrity of the government information in its possession. In addition, Contractor shall apply security controls when the Contractor reasonably determines that safeguarding requirements, in addition to those identified in paragraph (c) of this clause, may be required to provide adequate security, confidentiality and integrity in a dynamic environment based on an assessed risk or vulnerability. Contractor shall comply fully with all current and future updates of the information security requirements of PEBA, as outlined in this Contract and as provided during the term of the Contract.

(c) *Safeguarding requirements and procedures.* Contractor shall apply the following basic safeguarding requirements to protect government information from unauthorized access and disclosure:

(1) Protecting information on public computers or Web sites: Do not process government information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Government information shall not be posted on Web sites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (versus the Web site itself or the application it hosts).

(2) Transmitting electronic information. Transmit email, text messages, blogs, and similar communications that contain government information using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.

(3) Transmitting voice and fax information. Transmit government information via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients.

(4) Physical and electronic barriers. Protect government information by at least one physical and one electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(5) Sanitization. At a minimum, clear information on media that have been used to process government information before external release or disposal. Overwriting is an acceptable means of clearing media in accordance with National Institute of Standards and Technology 800–88, Guidelines for Media Sanitization, at [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf).

(6) Intrusion protection. Provide at a minimum the following protections against intrusions and compromise:

(i) Current and regularly updated malware protection services, e.g., anti-virus, antispyware.

(ii) Prompt application of security-relevant software upgrades, e.g., patches, service packs, and hot fixes.

(7) Transfer limitations. Transfer government information only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause.

(d) *Subcontracts.* Any reference in this clause to Contractor also includes any subcontractor at any tier. Contractor is responsible for, and shall impose by agreement requirements at least as secure as those imposed by this clause on, any other person or entity that contractor authorizes to take action related to government information.

(e) *Due Diligence.* Contractor shall complete a due diligence process annually or as otherwise requested by PEBA or a PEBA designated third party. This process may include a written questionnaire and, in some cases, could require an onsite visit from PEBA or a PEBA designated third party.

(f) *Background Checks.* Contractor shall ensure its staff shall have a criminal background check completed prior to accessing systems and/or applications that contain PEBA data. The background check shall be nationwide and, at a minimum, include federal, state, and county records where the Contractor's staff member has resided for the

past seven years. PEBA maintains the right to request a third party vendor or an individual who is involved with PEBA data and/or systems be removed from the further interaction with PEBA's data and/or systems.

(g) *Training.* Contractor shall provide security and privacy training, at least annually, for all staff members who have access to systems and/or applications that contain PEBA data.

(h) *Other contractual requirements regarding the safeguarding of information.* This clause addresses basic requirements and is subordinate to any other contract clauses or requirements to the extent that it specifically provides for enhanced safeguarding of information or information systems.

## **Replace with Clause 7.40 INFORMATION SECURITY - SAFEGUARDING REQUIREMENTS (FEB 2015)**

### **7.40 INFORMATION SECURITY - SAFEGUARDING REQUIREMENTS (FEB 2015)**

(a) *Definitions.* The terms used in this clause shall have the same meaning as the terms defined in the clause titled Information Security – Definitions. In addition, as used in this clause—

**Clearing** means removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

**Intrusion** means an unauthorized act of bypassing the security mechanisms of a system.

**Media** means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, large scale integration memory chips, and printouts (but not including display media, e.g., a computer monitor, cathode ray tube (CRT) or other (transient) visual output) onto which information is recorded, stored, or printed within an information system.

**Safeguarding** means measures or controls that are prescribed to protect information.

**Voice** means all oral information regardless of transmission protocol.

(b) *Safeguarding Information.* Without limiting any other legal or contractual obligations, Contractor shall implement and maintain reasonable and appropriate administrative, physical, and technical safeguards (including without limitation written policies and procedures) for protection of the security, confidentiality and integrity of the government information in its possession. In addition, Contractor shall apply security controls when the Contractor reasonably determines that safeguarding requirements, in addition to those identified in paragraph (c) of this clause, may be required to provide adequate security, confidentiality and integrity in a dynamic environment based on an assessed risk or vulnerability. Contractor shall comply fully with all current and future updates of the information security requirements of PEBA, as outlined in this Contract and as provided during the term of the Contract.

(c) *Safeguarding requirements and procedures.* Contractor shall apply the following basic safeguarding requirements to protect government information from unauthorized access and disclosure:

(1) Protecting information on public computers or Web sites: Do not process government information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Government information shall not be posted on Web sites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (versus the Web site itself or the application it hosts).

(2) Transmitting electronic information. Transmit email, text messages, blogs, and similar communications that contain government information using technology and processes that provide industry standard (as approved by PEBA) level of security and privacy available, given facilities, conditions, and environment.

(3) Transmitting voice and fax information. Transmit government information via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients.

- (4) Physical and electronic barriers. Protect government information by at least one physical and one electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
- (5) Sanitization. At a minimum, clear information on media that have been used to process government information before external release or disposal. Overwriting is an acceptable means of clearing media in accordance with National Institute of Standards and Technology 800–88, Guidelines for Media Sanitization, at [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf).
- (6) Intrusion protection. Provide at a minimum the following protections against intrusions and compromise:
- (i) Current and regularly updated malware protection services, e.g., anti-virus, antispyware.
  - (ii) Prompt application of security-relevant software upgrades, e.g., patches, service packs, and hot fixes.
- (7) Transfer limitations. Transfer government information only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause.
- (d) *Subcontracts*. Any reference in this clause to Contractor also includes any subcontractor at any tier. Contractor is responsible for, and shall impose by agreement requirements at least as secure as those imposed by this clause on, any other person or entity that contractor authorizes to take action related to government information.
- (e) *Due Diligence*. Contractor shall complete a due diligence process annually or as otherwise requested by PEBA or a PEBA designated third party. This process may include a written questionnaire and, in some cases, could require an onsite visit from PEBA or a PEBA designated third party.
- (f) *Background Checks*. Contractor shall ensure its staff shall have a criminal background check completed prior to accessing systems and/or applications that contain PEBA data. The background check shall be nationwide and, at a minimum, include federal, state, and county records where the Contractor’s staff member has resided for the past seven years. PEBA maintains the right to request a third party vendor or an individual who is involved with PEBA data and/or systems be removed from the further interaction with PEBA’s data and/or systems.
- (g) *Training*. Contractor shall provide security and privacy training, at least annually, for all staff members who have access to systems and/or applications that contain PEBA data.
- (h) *Other contractual requirements regarding the safeguarding of information*. This clause addresses basic requirements and is subordinate to any other contract clauses or requirements to the extent that it specifically provides for enhanced safeguarding of information or information systems.

**All other terms and conditions remain unchanged.**