Request for Proposals

for

Service Organization Controls 1 and 2 Reporting Services

for the

Retirement Systems of Alabama

and the

Public Education Employees' Health Insurance Plan

for

Fiscal Years 2024, 2025, 2026, 2027, and 2028

RFP 23-0003

THIS RFP CONTAINS INFORMATION UNDER THE FOLLOWING HEADINGS:

Section I - General Information for the Proposer

A. Purpose
B. Description of the Retirement Systems of Alabama & the Public Education Employees' Health Insurance Plan
C. Other Information
D. Proposal Timetable
E. Delivery Schedule
F. Payment Schedule
G. Contact Point
H. Minimum Qualifications

Section II - Information Required from Proposers

A. Qualifications of the Firm
B. Technical Proposal
C. Cost Proposal

Section III - Criteria for Evaluation

A. General
B. Cost & Price Analysis
C. Proposal Evaluation Form

Section IV – Additional Documents

A. State of Alabama Disclosure Statement (Pursuant to the *Code of Alabama 1975, Title 41, Chapter 16, Article 3B)*
B. Sample RSA State Contract
C. Immigration Compliance Certificate
D. Bidder Profile Form
E. Bidder References Form
F. Confirmation of Review of PEEHIP Statement on HIPAA Compliance Documentation
G. HIPAA Compliance Questions
H. Sample Business Associate Agreement
I. IRS Form W-9
J. Certification of Bidder or Proposer
K. Non-Disclosure Agreement
L. E-Verify Memorandum of Understanding

Section I – General Information for the Proposer

A. Purpose

This Request For Proposals (RFP) solicits vendor proposals for the following reports:

1. Report on Management's Description of Retirement Systems of Alabama's System and the Suitability of the Design and Operating Effectiveness of Controls—Type 2 SOC 1
2. Report on Management's Description of Retirement Systems of Alabama's PEEHIP Benefits Administration System and the Suitability of the Design and Operating Effectiveness of Controls—Type 2 SOC 1
3. Report of Retirement Systems of Alabama's Description of Its Data Center Hosting Services System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Processing Integrity, and Confidentiality—Type 2 SOC 2.

These reports shall be prepared for each of fiscal years 2024, 2025, 2026, 2027, and 2028, and shall be prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 21.* Type 2 SOC 1 reports should particularly focus on the areas of investment transactions and cycle, member contributions and reporting, member retirement/withdrawal disbursement and participant data. RSA will also require the SOC 3 report for the Type 2 SOC 1 report.

B. Description of RSA & PEEHIP

Introduction

The Teachers' Retirement System (TRS), the Employees' Retirement System (ERS), and the Judicial Retirement Fund (JRF) are collectively referred to as The Retirement Systems of Alabama (RSA). As directed by state law, RSA also manages and administers the Public Education Employees' Health Insurance Plan (PEEHIP) and the RSA-1 Deferred Compensation Plan (RSA-1). For purposes of this RFP, unless the intent is clearly otherwise, the term "RSA" shall include PEEHIP and RSA-1.

The TRS, a cost-sharing multiple-employer public employee retirement plan, was established as of September 15, 1939, pursuant to the *Code of Alabama 1975, Title 16, Chapter 25* (Act 419 of the Legislature of 1939) for the purpose of providing retirement allowances and other specified benefits for qualified persons employed by State-supported educational institutions. The responsibility for the general administration and operation of the TRS is vested in its Board of Control.

The ERS, an agent multiple-employer public employee retirement plan, was established as of October 1, 1945, pursuant to the *Code of Alabama 1975, Title 36, Chapter 27* (Act 515 of the Legislature of 1945). The purpose of the ERS is to provide retirement allowances and other specified benefits for state employees, State Police, and, on an elective basis, to all cities, counties, towns, and quasi-public organizations. Assets of the ERS are pooled for investment purposes. However, separate accounts are maintained for each individual employer so that each employer's share of the pooled assets is legally available to pay the benefits of its employees only. The responsibility for the general administration and operation of the ERS is vested in its Board of Control.

The JRF, a cost-sharing multiple-employer public employee retirement plan, was established as of September 18, 1973, pursuant to the *Code of Alabama 1975, Title 12, Chapter 18* (Act 1163 of the Legislature of 1973) for the purpose of providing retirement allowances and other specified benefits for any Justice of the Supreme Court of Alabama, Judge of the Court of Civil Appeals, Judge of the Court of Criminal Appeals, Judge of the Circuit Court, or office holder of any newly created judicial office receiving compensation from the State Treasury. The *Code of Alabama 1975, Title 12, Chapter 18, Articles 3 & 4* (Act 1205 of the Legislature of 1975) enlarged the scope and coverage of the JRF to include District and Probate Judges, respectively. The responsibility for the general administration and operation of the JRF is vested in the Board of Control of the ERS.

The PEEHIP was established in 1983 pursuant to the *Code of Alabama 1975, Title 16, Chapter 25A* (Act 83-455 of the Alabama Legislature) to provide a uniform plan of health insurance for active and retired employees of state and local educational institutions which provide instruction at any combination of grades K-14 (collectively, eligible employees), and to provide a method for funding the benefits related to the plan. The four-year universities participate in the plan with respect to their retired employees and are eligible and may elect to participate in the plan with respect to their active employees. Responsibility for the establishment of the health insurance plan and its general administration and operations is vested in the Public Education Employees' Health Insurance Board. The Board is a corporate body for purposes of management of the health insurance plan. The Board has been appointed as the administrator of the PEEHIP.

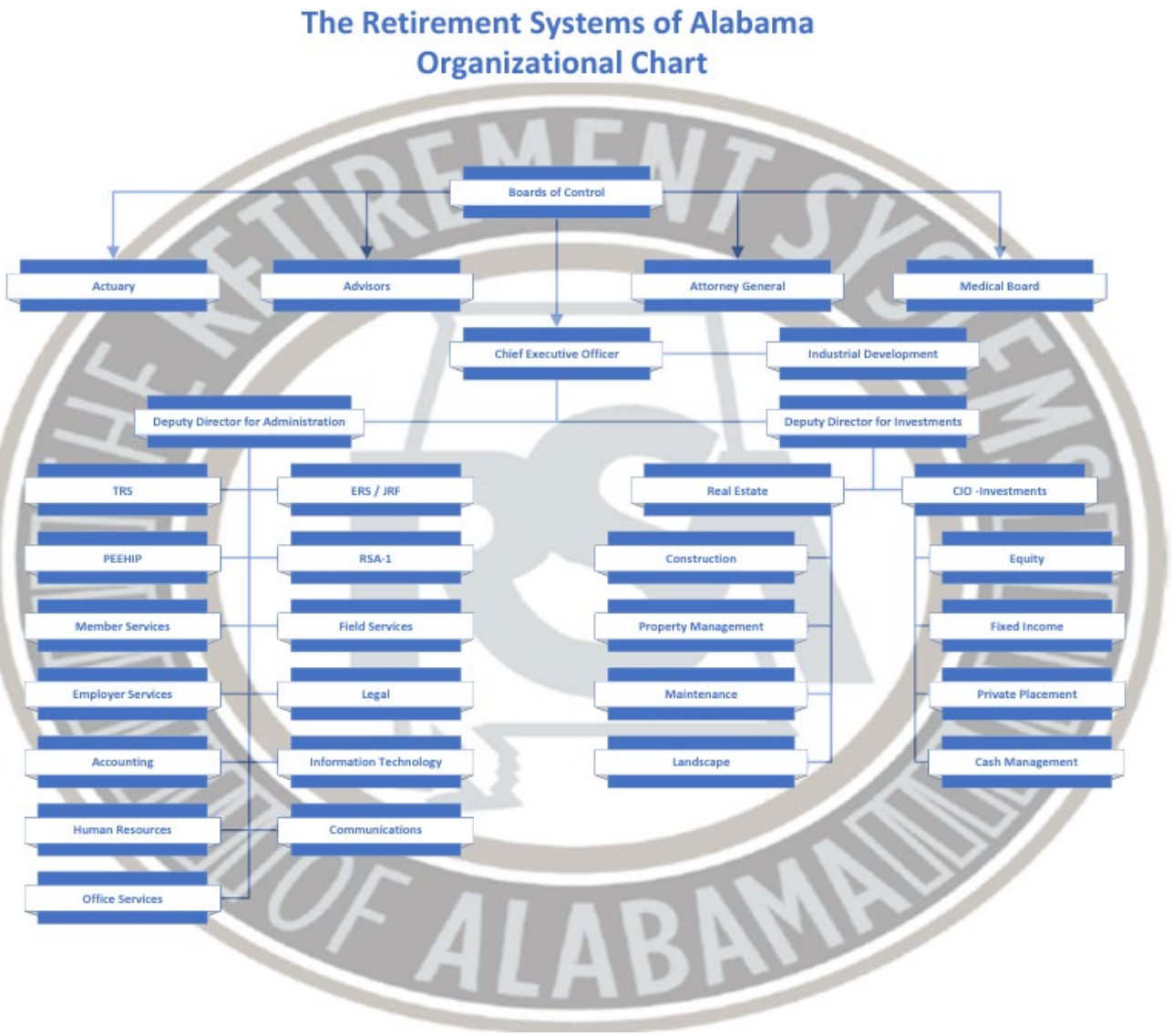
The Alabama Retired Education Employees' Health Care Trust (Trust) is a cost-sharing multiple-employer defined benefit postemployment healthcare plan that administers healthcare benefits to the retirees of participating state and local educational institutions. The Trust was established under the Alabama Retiree Health Care Funding Act of 2007 which authorized and directed the Public Education Employees' Health Insurance Board (Board) to create an irrevocable trust to fund postemployment healthcare benefits to retirees. Active and retiree health insurance benefits are paid through the Public Education Employees' Health Insurance Fund (PEEHIF). In order to comply with the reporting requirements of Governmental Accounting Standards Board (GASB) Statement No. 74, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans*, the contributions and benefit payments related to retirees that are processed through the PEEHIF are segregated from the PEEHIF and reported as part of the Trust.

RSA-1 was established as of November 26, 1986, under the provisions of the *Code of Alabama 1975, Title 36, Chapter 27A* (Act 685 of the Legislature of 1986). RSA-1 operates as a deferred compensation plan as defined in Section 457 of the Internal Revenue Code of the United States and began receiving deferred portions of employees' income on January 1, 1987. The responsibility for the general administration and operation of RSA-1 is vested in its Board of Control which is made up of the TRS and ERS Investment Committee members. All members of TRS, ERS, JRF, and employees of employers eligible to participate in the ERS pursuant to provisions of the *Code of Alabama 1975, Title 36, Chapter 27, Article 6*, and public officials and employees of the State of Alabama or any political subdivision thereof (collectively, participating employers) are eligible to participate.

RSA provides the following administrative and support services to all the plans described above: Legal, Investments, Accounting, Information Technology, Human Resources, Office Services, Property Management & Maintenance, Field Services, Member Services, Employer Services and Communications.

Organization

The following is a summary of the major organizational roles at the RSA and is intended to provide a general overview of the organization and does not include all groups or activities. An organizational chart of the RSA is shown below and is followed by narrative descriptions of the various divisions.



Chief Executive Officer

The CEO is appointed by the Boards of Control to administer the various RSA programs and to manage the day-to-day operations of the RSA. This includes overall decision-making authority over all the aspects of the RSA operations.

Deputy Directors

The Deputy Director for Administration and Deputy Director for Investments answer directly to the CEO and oversee the core business operations of the RSA.

Legal

The Legal Division provides legal advice to all RSA divisions, reviews and interprets governing statutes and regulations, offers counsel to the governing boards, reviews contracts entered into by the RSA, defends and prosecutes lawsuits, assists with the appeal process of both administrative and statutory denials, and assures compliance with any fiduciary obligations. The Division includes Legislative Counsel, who monitors legislation that could have an impact on the RSA, provides guidance to the RSA personnel, and represents the RSA to the Legislature. There are five employees within the division.

Investments

The Investment Division's major function is to optimize the total return on RSA's investment portfolio through a policy of long-term diversified investment, using parameters of prudent risk management. The RSA Investments personnel administers and monitors the RSA investments, coordinates the RSA cash flow, implements the asset allocation strategy, and monitors and reports on investment activity and performance. Each member of the Investments division generally focuses on a certain asset class, with consideration given to how their recommendations affect the overall portfolio. There are both passive and active strategies employed within equities, and the entire fixed income portfolio is actively managed. Direct investments are also part of the RSA investment strategy and consist of both equity and debt investments. There are thirteen employees within this division.

Benefits Division

The primary function of the Benefits Division is to calculate and process all retirement, disability, death, and refund claims. Benefits personnel also administer and maintain recurring benefits, return to work, beneficiary information, and provides counseling, guidance, and education to the RSA members (active, inactive, and retired), their beneficiaries, and employers. To provide these services, personnel must be knowledgeable of the Alabama law as it pertains to all participating employers and be able to explain how it affects members and employers. When needed, Benefits personnel serve as a liaison between the member and employer and the RSA. There are seventy-five employees within the division.

PEEHIP Division

The Public Education Employees' Health Insurance Plan (PEEHIP) provides quality healthcare insurance benefits for public education employees and retirees. PEEHIP personal administer open enrollment, eligibility and changes during the year. Accounting staff process billing, receipts, and preparation of financial statements, budgets and projections. There are 26 employees in the division.

RSA-1 Division

The primary function of the RSA-1 Division is to process enrollment and disbursements for the Section 459(b) plan. RSA-1 personnel also administer and maintain recurring benefits, beneficiary information, and provides counseling, guidance, and education to the RSA-1 members (active, inactive, and retired), their beneficiaries, and employers. To provide these services, personnel must be knowledgeable of Federal law as it pertains to Section 459(b) plans and be able to explain how it affects members. There are 12 employees within the division.

Accounting Division

The Accounting Division has several functional areas with varying responsibilities related to accounting and financial reporting as described below. There are fifty-three employees in the Accounting Division.

1) CFO-Accounting
   - Oversees the accounting Division as a whole
   - Monitors internal controls for the entire organization and all related entities
   - Develops and implements strategies related to PEEHIP funding
   - Prepares the Budget Requests for RSA and all related entities
   - Tests all participant and employer data and provides it to the actuary for the annual actuarial valuations
   - Manages Financial Analysis area which provides data analysis in support of decisions as well as process improvement implementations.

2) Financial Reporting
   - Prepares RSA's Annual Comprehensive Financial Report (ACFR) for TRS, ERS & JRF
   - Prepares audited financial statements for RSA-1 & PEIRAF and any other external financial reporting
   - Analyzes the general ledger to ensure entries are posted to the correct accounts

3) Investment Accounting
   - Managing and projecting cash needs
   - Works closely with Investment personnel, brokerage firms, traders, the State Treasurer, the State Comptroller, and the custodial bank
   - Recording the daily investment activity and settling all trading activity
   - Acquiring and retaining all required authorizations related to trading of securities and cash movements
   - Reconciling to the custodial bank, the in-house investment accounting software, and the general ledger for all investment activity the investments of the RSA are 100% internally managed
   - Responsible for the investment activity for 24 funds with investments valued at approximately $43.9 billion at September 30, 2022
   - Investments include Short-Term Investment Funds, Commercial Paper, Domestic Fixed Income & Equity Securities, International Equity Securities, Direct Private Placement Investments, and Directly owned and managed Real Estate Investments
   - Investment performance is calculated and reported by the third-party custodial bank

4) Revenue Accounting
   - Responsible for collecting, balancing, and posting the employee and employer contributions for TRS, ERS, JRF, RSA-1, and PEEHIP
   - Calculate investment earnings and post to members' accounts
   - Producing quarterly statements for RSA-1 and PEIRAF
   - Balances member account detail from the subsidiary ledger to the general ledger for, RSA-1 and PEIRAF

5) Member Payroll
   - Verifies and balances the monthly retirement payroll for approximately 142,000 recipients
   - Processes one daily and two weekly ad hoc payrolls
   - Balances the 1099 file to the check distributions and general ledger

6) Accounting Operations
   - Responsible for all aspects of the accounts payable function for RSA
   - Maintains detail of various general ledger accounts to ensure entries are posted correctly and timely
   - Prepares the annual Operations Plans for the expense funds of TRS, ERS, JRF, and PEEHIP
   - Prepares Audited Financial Statements for PEEHIP and Retiree Healthcare Trust
   - Prepares financial statements for Real Estate and Construction projects

Information Technology Division

The IT Division provides technology solutions which enable superior customer service to members, employers, and annuitants. IT maintains an integrated Microsoft Windows-based file/application server, web, imaging, and telecommunications infrastructure, assures a high level of information security and disaster recovery readiness, and ensures support to changing business needs and legislative changes. The Chief Security Officer (CSO) is responsible for assuring the confidentiality, integrity, and availability of information and information systems throughout the organization. The CSO ensures that appropriate technology monitoring and controls are in place. There are fifty-five people in this division.

Human Resources

The Human Resources Division is responsible for administering all human resource functions for the organization. This includes recruitment, employment practices, benefits and compensation, and management policies. They also are responsible for personnel training and development. There are four people in this division.

Office Services

The Office Services Division is responsible for handling incoming mail and processing outgoing mail. Office Services personnel scans incoming paper documents into the imaging system in order for them to be entered into workflow or stored. This area also enters address inactive members and retirees. Office Services is responsible for purchasing any equipment or supplies necessary for conducting business and ensuring the proper maintenance of the equipment. In-house printing and binding services are also available through Office Services. There are nine people within the division.

Property Management / Maintenance

This division is responsible for construction and/or management of the various real estate investment properties owned by RSA. This includes marketing vacant office spaces, negotiating, executing, and monitoring appropriate contracts and leases, maintaining tenant relations, tenant building improvements, providing support to tenants including telecommunications and IT, and maintaining both the interior and exterior of the buildings and the surrounding grounds. There are eighteen people within the division.

Field Services

The Field Services Division conducts an ongoing series of educational seminars for TRS and ERS members in order to better educate participants of their retirement benefits. They also provide informational programs on PEEHIP hospital medical and other PEEHIP available coverages, the RSA-1 Deferred Compensation Plan, and the Flex savings program. There are six people within that division.

Member Services

The Member Services Division serves as the initial point of contact for members of RSA, their beneficiaries, and other financial professionals. The primary function of employees in Member Services is receiving and filtering incoming telephone inquiries. After assessing the nature of each inquiry, personnel then provide general plan information and/or necessary documents or forwards the more technical inquiries to the appropriate division. Member Services also receives, filters, responds to, or forwards incoming email and written inquires. All contact, regardless of the type, should be documented in the member files for review and/or future reference. Member Services also manages the visitor center for members with appointments or those who may walk-in to see an RSA Benefits Counselor. Visitor center personnel assess the reason for member visits and may either assist visitors with general plan inquiries by providing both information and plan documents or schedule a session with a benefits counselor. The visitor center personnel also accept, receive, and forward to the correct party member payments for various plans. There are nineteen people within this division.

Employer Services

The Employer Services Division serves as the primary contact point for employers regarding questions relating to member enrollment, employer enrollment and contribution reporting. Employer Service Representatives will assist employers regarding correct member data, sick leave participation and reporting, payroll and personnel reporting requirements, time deadlines and required documentation submission, proper member retirement tier assignment, class assignment and contribution payment type, as well as provide information on plan program eligibility, and membership rights and obligations. There are nine people within this division.

Communications

The Communications Division provides information to the general public, employers, and members regarding RSA. They create forms, newsletters, benefit booklets, manuals, and correspondence for members and employers, as well as technical manuals and training materials for RSA employees. In addition, Communications personnel develops content for and maintains RSA's public website as well as an intranet for RSA personnel. There are three people within the division.

C. Other Information

Other documents that are considered as part of this RFP may be located via the internet as follows:

Additional Terms and Conditions applicable to, and deemed incorporated within, this RFP and all proposals submitted in response to this RFP – https://www.rsa-al.gov/about-rsa/itb-rfp/

1. RSA Reservations of Rights and Requirements for ITBs and RFPs
2. RSA Standard Terms and Conditions for Solicitations and Contracts

Please Note: By submitting a proposal, all proposers will be deemed to have agreed to all terms and conditions included within the above documents unless a proposer provides RSA with a document clearly stating its exceptions to any term or condition, along with a detailed justification therefor.

RSA Website – www.rsa-al.gov

1. RSA Annual Comprehensive Financial Report (ACFR) – 2022
2. TRS Summary Plan Description
3. ERS Summary Plan Description
4. Member Handbooks for TRS, ERS, State Police, JRF, and PEEHIP
5. RSA-1 Publications
6. PEEHIP Publications

Alabama Secretary of State Website – www.sos.alabama.gov

1. TRS Law – *Code of Alabama 1975, Title 16, Chapter 25*
2. ERS Law – *Code of Alabama 1975, Title 36, Chapter 27*
3. JRF Law – *Code of Alabama 1975, Title 12, Chapter 18*
4. PEIRAF Law – *Code of Alabama 1975, Title 36, Chapter 27A*
5. PEEHIP Law – *Code of Alabama 1975, Title 16, Chapter 25A*
6. PEEHIP Retiree Trust Law – Legislative Act 2007-16

D. Proposal Timetable

The following timeline shall apply to this RFP. RSA reserves the right to adjust this schedule as it deems necessary or in RSA's best interest at any point during the solicitation process. Notification of any adjustment to this timeline will be posted on RSA's website (https://www.rsa-al.gov/about-rsa/itb-rfp/), except that RSA may adjust the Contract Award date in its sole discretion without posting any notification of adjustment on RSA's website.

Proposal issued and posted to RSA's website	**July 31, 2023**
Deadline for receipt of questions	**August 7, 2023, 2:00 p.m. CST**
Responses to questions posted to RSA's website	**August 11, 2023, 2:00 p.m. CST**
Proposals Due	**September 1, 2023, 2:00 p.m. CST**
Finalist Interviews	**September 18-22, 2023**
Award Contract	**September 25, 2023**

All proposals will be submitted (six (6) copies) in a sealed wrapper with the following plainly marked on the front:

RETIREMENT SYSTEMS OF ALABAMA
SOC AUDIT PROPOSAL
RFP 23-0003
OPENING September 1, 2023

In addition to the six physical copies of your proposal, you must provide your proposal in electronic format. We also request a redacted physical copy and in electronic format.

Proposals sent via FedEx or UPS:

Mr. Taylor Benefield
Retirement Systems of Alabama
201 South Union Street
Montgomery, Alabama 36104

Proposals sent via U.S. Mail:

Mr. Taylor Benefield
Retirement Systems of Alabama
PO Box 302150
Montgomery, Alabama 36130-2150

Proposals may be hand delivered to Room 574 of the Retirement Systems Building, 201 South Union Street, Montgomery, Alabama. Proposals will be accepted until 2:00 p.m. CST on September 1, 2023. Proposals will not be accepted after this time.

E. Delivery Schedule

Selected firm must be prepared to begin engagement no later than February 1, 2024. All reports must be completed and issued by November 30 of each year for the previous fiscal year. RSA's fiscal year end is September 30.

F. Payment Schedule

Payment will be made based upon submitted invoices for work performed during the period. Invoices may not be submitted more frequently than monthly. Payment will be made within 30 days of receipt of the invoice.

G. Contact Point

Any questions that arise concerning this RFP may be directed to Mr. Taylor Benefield at Taylor.Benefield@rsa-al.gov.

H. Minimum Qualifications

Proposals will be accepted from public accounting firms where both the firm and the assigned personnel meet the following minimum qualifications:

- Audit Manager/Partner on this engagement must possess a current Certified Information Systems Auditor certification and must have at least five years of experience combined in SOC 1 and 2 reporting.
- All firm personnel assigned to the engagement must sign a non-disclosure & confidentiality agreement.
- Furnish resumes for primary persons responsible for the engagement reflecting relevant experience.
- Furnish references from a minimum of three clients for whom the firm has completed SOC 1 Type 2 and SOC 2 Type 2 reports

Section II – Information Required from Proposers

Proposals must be submitted in the format outlined below:

A. Qualifications of the Firm

1. Business Organization

State the full name and address of your organization, and if applicable, the branch office or other subordinate element that will perform or assist in performing the work hereunder. Indicate whether you operate as an individual, partnership, or corporation; if as a corporation, include the state in which you incorporated. State whether you are licensed to operate in the State of Alabama.

2. Background Information

Disclose any disciplinary action or litigation taken within the last five years against the firm or firms' staff regarding professional services or breach of a contract to provide services. Describe any relationships your firm or staff may have with the RSA or another affiliated company that could represent a conflict of interest.

3. Prior Experience

As part of your proposal, include a brief statement (maximum of five pages) concerning the relevant experience of persons from your firm who will be associated at the highest management levels with the proposed engagement. Do not include general corporate background brochures. Emphasize experience directly applicable to SOC 1 Type 2 and SOC 2 Type 2 reporting.

4. Personnel

Identify lead individuals by name and title and include a resume of each.

5. Authorized Officials

Include the names and telephone numbers of personnel authorized to execute the proposed contracts with the RSA.

6. Personally Identifiable Information

Describe any policies, procedures, and/or training that your firm has in place or your employees have attended regarding the security of client information.

7. Additional Information and Comments

Include any other information believed to be pertinent but not specifically requested elsewhere in this RFP.

B. Technical Proposal

Prepare a description of the approach you anticipate following in critical audit areas. Specifically discuss your methodology utilizing a readiness approach, timing of the engagement, estimated number of hours, and estimated client involvement. Also, describe your process for client submitting supporting documentation. RSA requires all final reports to be issued no later than November 30 after each fiscal year end.

C. Cost Proposal

Proposal must include a pricing model for completion of two SOC 1 Type 2 reports and one SOC 2 Type 2 reports (including SOC 3 report) as described earlier in this RFP. The information requested in this Section is required to support the reasonableness of your proposal price. Your proposal must include a Fee Schedule for fiscal years 2024, 2025, 2026, 2027, and 2028 including a total for the entire 5-year contract period. Please provide the Fee Schedule in the following format:

Fiscal Year – 10/1 to 9/30	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028
Hourly Rate	$ XXX	$XXX	$XXX	$XXX	$XXX
Staff Title/Role	Projected Hours per Staff				
Example Staff #1	XXX	XXX	XXX	XXX	XXX
Example Staff #2	XXX	XXX	XXX	XXX	XXX
Example Staff #3	XXX	XXX	XXX	XXX	XXX
Example Staff #4	XXX	XXX	XXX	XXX	XXX
Example Staff #5	XXX	XXX	XXX	XXX	XXX
Total Hours	XXX	XXX	XXX	XXX	XXX
Total Estimated Fees	$X,XXX	$X,XXX	$X,XXX	$X,XXX	$X,XXX

Section III – Criteria for Evaluation

A. General

The following process will be used to evaluate vendor proposals:

a. A review committee will evaluate each proposal submitted in response to these Proposal specifications.
b. Responses received within the time frame and in the form specified by the guidelines will first be evaluated to confirm that all proposal sections, as detailed, have been provided in the Proposal response.
c. Each proposal will be reviewed and points awarded to all items on the Proposal Evaluation Form. A proposal component may be awarded points not to exceed the maximum specified. The total technical score available is 70 points.
d. Each proposal component will be summed to obtain a total score.
e. RSA may conduct interviews with the finalists.

B. Cost & Price Analysis

The cost evaluation will be based on an examination by the Evaluation Committee of each Proposer's stated cost components and will constitute 30% of the overall proposal's evaluation. The preparation of your reports should be a fixed price. Billing is to be submitted with the detail, by staff member, of hours worked on each task. The total paid to the selected vendor for your reports will not exceed the proposed cost unless both parties agree in writing.

Cost scoring will be determined as follows:

a. Cost proposals must be provided in a separate envelope clearly labeled "Cost Proposal."
b. The Proposer submitting the lowest cost Proposal will receive 30 points.
c. All other Proposers will be evaluated by use of the following formula:

$$\frac{\text{Lowest Cost of All Proposals}}{\text{Cost of Proposal Under Evaluation}} \times 30 \text{ points} = \text{Proposer's Score for Cost Proposal}$$

RSA & PEEHIP are not liable for any expense for use of a job classification by the proposer not identified in the proposer's response.

C. Proposal Evaluation Form

General Proposal Categories	Possible Points	Reviewer's Score
Description of Services to be Performed	10	
Experience with Similar Proposals	20	
Experience of Personnel Assigned	20	
IT Risk	10	
Methodology and Ability to Meet Timeline	10	
Total Technical Score	**70**	
Cost Proposal	30	
Total Possible Points	**100**	

Proposers must respond to all required components of the RFP.

Finalist Interviews will allow for a possible additional 10 points.

Section IV – Additional Documents

The following documents must be completed and submitted with your proposal. These documents may be found on the RSA website (https://www.rsa-al.gov/about-rsa/itb-rfp/). RSA may, at its discretion, reject any proposal not containing all of the requested additional documents.

A. State of Alabama Disclosure Statement (Pursuant to the *Code of Alabama 1975, Title 41, Chapter 16, Article 3B)*

B. Sample RSA State Contract – This document does not have to be signed; however, proposers must document any exceptions to the standard terms or will be deemed to have accepted all standard terms contained in this sample contract.

C. Immigration Compliance Certificate

D. Bidder Profile Form

E. Bidder References Form

F. Confirmation of Review of PEEHIP Statement on HIPAA Compliance Documentation

G. HIPAA Compliance Questions

H. Sample Business Associate Agreement – This document does not have to be signed with the return of the proposal; however, proposers must document any exceptions to the standard terms or will be deemed to have accepted all standard terms contained in this sample BAA.

I. IRS Form W-9

J. Certification of Bidder or Proposer

K. Non-Disclosure Agreement – This document does not have to be signed with the return of the proposal; however, proposers must document any exceptions to the standard terms or will be deemed to have accepted all terms contained in this NDA.

L. E-Verify Memorandum of Understanding – A copy of the proposer's fully-executed E-Verify MOU with the US Department of Homeland Security should be included with your proposal.

STATE OF ALABAMA
MONTGOMERY COUNTY

AGREEMENT TO PROVIDE PROFESSIONAL SERVICES

THIS AGREEMENT TO PROVIDE PROFESSIONAL SERVICES, which results from RSA RFP _____, entitled Request for Proposals for _____, is made and entered into effective _____, 2023, by and between the Teachers' Retirement System of Alabama, the Employees' Retirement System of Alabama, and the Judicial Retirement Fund, collectively known as The Retirement Systems of Alabama ("RSA"), and _____, hereinafter referred to as "Contractor".

RECITALS

A. RSA issued an RFP for _____ (describe services), and Contractor was awarded this contract based upon the terms of Contractor's Proposal dated _____, 2023 ("Contractor's Proposal").

B. The parties wish to enter into this Agreement to formalize the terms under which Contractor will provide the services.

Now, Therefore, in consideration of the foregoing and the mutual covenants of the parties contained herein, the receipt and sufficiency of which are acknowledged, the parties agree as follows:

1. Scope of Services. Upon request of RSA, Contractor shall perform the following services for RSA ("Services"): _____.

2. Consideration. As consideration for the Services rendered pursuant to this Agreement, RSA agrees to compensate Contractor in accordance with the rates and fees set forth in Exhibit A, which is attached hereto and incorporated herein by reference.

Contractor shall send detailed invoice(s) for all work in arrears as work is completed but no more frequently than monthly. RSA shall have thirty days from receipt of an invoice from Contractor to render payment. Should RSA dispute any invoiced amount, RSA must deliver within thirty days of receipt of invoice written notice to Contractor detailing the specific facts and circumstances of the dispute and shall timely pay all undisputed amounts. The parties agree to work together in good faith to resolve any disputed amounts.

The maximum compensation due to Contractor during the term of the Agreement shall not exceed _____.

3. Term. This Agreement shall be for the period beginning _____, 2023, and ending _____, _____.

4. Approvals. Contractor acknowledges and understands that this Agreement is not effective until it has received all required state government approvals, and Contractor shall not begin performing work hereunder until notified to do so by RSA. Contractor is entitled to no compensation for work performed prior to the effective date of this Agreement.

5. Independent Contractors. Contractor acknowledges that Contractor is an independent contractor, and neither Contractor nor Contractor's employees are to be considered employees of RSA or entitled to benefits under the State of Alabama merit system.

6. **No State Debt, Etc.** Contractor acknowledges that the terms and commitments contained herein shall not be constituted a debt of the State of Alabama in violation of Article 11, Section 213 of the Constitution of Alabama, 1901, as amended by Amendment Number 26. It is further agreed that if any provisions of this Agreement shall contravene any statute or Constitutional provision or amendment, either now in effect or which may, during the course of the Agreement, be enacted, then that conflicting provision in the Agreement shall be deemed null and void and the remaining provisions shall continue to be valid and enforceable. Contractor may not assign this Agreement or any interest herein or any money due hereunder without the expressed written consent of RSA.

7. **Indemnification.** To the fullest extent permitted by law, the Contractor shall defend, indemnify, and hold harmless RSA, and their agents and employees (hereinafter collectively referred to as the "Indemnitees") from and against all claims, damages, losses and expenses, including but not limited to attorneys' fees, arising out of, related to, or resulting from performance of the Services, provided that such claim, damage, loss or expense is caused in whole or in part by negligent acts or omissions of the Contractor, a subcontractor of Contractor, anyone directly or indirectly employed by them, or anyone for whose acts they may be liable, regardless of whether such claim, damage, loss or expense is caused in part, or is alleged but not legally established to have been caused in whole or in part by the negligence or other fault of a party indemnified hereunder. This indemnification does not apply to the extent of the sole negligence of the Indemnitees.

8. **Insurance.** Contractor agrees that Contractor shall maintain or obtain (as applicable), with respect to the activities in which Contractor engages pursuant to this Agreement, general liability insurance, workers compensation insurance, automobile liability insurance, cyber security insurance, and professional liability (errors and omissions) insurance, in amounts reasonable and customary for the nature and scope of business engaged by Contractor. All insurance shall be provided by insurers licensed in Alabama, or in the state where Contractor resides, to provide the types of insurance required, and insurers must be rated "A-"or better by the A.M. Best Company. Before beginning work, Contractor shall have on file with RSA a valid Certificate of Insurance showing the types and limits of insurance carried. The foregoing coverages shall be maintained without interruption for the entire term of this Agreement. If requested by RSA, Contractor agrees to name RSA as additional insured on any applicable policies. RSA reserves the right to require additional insurance coverage other than that listed herein as RSA deems appropriate from time to time with a 30-day notice to Contractor.

Contractor must provide at least 30 days' notice (10 days' notice in the event of cancellation due to non-payment of premium) prior notice of any cancellation, non-renewal or material change to any insurance policy covered by this Agreement. If any such notice is given, RSA shall have the right to require that a substitute policy(ies) be obtained prior to cancellation and replacement Certificate(s) of Insurance shall be provided to RSA.

9. **Confidentiality and Ownership.** Contractor acknowledges that, in the course of performing its responsibilities under this Agreement, Contractor may be exposed to or acquire information that is proprietary or confidential to RSA or RSA's members. Contractor agrees to hold such information in confidence and not to copy, reproduce, sell, assign, license, market, transfer or otherwise disclose such information to third parties or to use such information for any purpose whatsoever, without the express written permission of RSA, other than for the performance of obligations hereunder or as required by applicable state or federal law. For purposes of this Agreement, all records, financial information,

specifications and data disclosed to Contractor during the term of this Agreement, whether submitted orally, in writing, or by any other media, shall be deemed to be confidential in nature unless otherwise specifically stated in writing by RSA.

Contractor acknowledges that all data relating to RSA is owned by RSA and constitutes valuable property of RSA. RSA shall retain ownership of, and all other rights and interests with respect to, its data (including, without limitation, the content thereof, and any and all copies, modification, alterations, and enhancements thereto, and any derivative works, resulting therefrom), and nothing herein shall be construed as granting Contractor any ownership, license, or any other rights of any nature with respect thereto. Contractor may not use RSA's data (including de-identified data) for any purpose other than providing the Services contemplated hereunder. Upon termination of the Agreement, Contractor agrees to return or destroy all copies of RSA's data in its possession or control except to the extent such data must be retained pursuant to applicable law.

10. State Immigration Law Compliance. By signing this Agreement, the contracting parties affirm, for the duration of the Agreement, that they will not violate federal immigration law or knowingly employ, hire for employment, or continue to employ an unauthorized alien within the State of Alabama. Furthermore, a contracting party found to be in violation of this provision shall be deemed in breach of the Agreement and shall be responsible for all damages resulting therefrom.

11. Boycott Prohibition. In compliance with Act 2016-312, Contractor hereby certifies that it is not currently engaged in, and will not engage in, the boycott of a person or an entity based in or doing business with a jurisdiction with which this state can enjoy open trade.

12. Dispute Resolution. In the event of any dispute between the parties, senior officials of both parties shall meet and engage in a good faith attempt to resolve the dispute. Should that effort fail and the dispute involves the payment of money, a party's sole remedy is the filing of a claim with the Board of Adjustment of the State of Alabama.

For any and all other disputes arising under the terms of this Agreement which are not resolved by negotiation, the parties agree to utilize appropriate forms of non-binding alternative dispute resolution including, but not limited to, mediation. Such dispute resolution shall occur in Montgomery, Alabama, utilizing where appropriate, mediators selected from the roster of mediators maintained by the Center for Dispute Resolution of the Alabama State Bar.

Contractor acknowledges and agrees that RSA is prohibited from indemnifying Contractor for any reason. RSA does not release or waive, expressly or impliedly, RSA's right to assert sovereign immunity or any other affirmative defense right it may have under state law. RSA shall control the defense and settlement of any legal proceeding on behalf of RSA, including the selection of attorneys.

13. Proration. Any provision of this Agreement notwithstanding, in the event of failure of RSA to make payment hereunder as a result of partial unavailability, at the time such payment is due, of such sufficient revenues of the State of Alabama or RSA to make such payment (proration of appropriated funds for the State of Alabama having been declared by the governor pursuant to Section 41-4-90 of the Code of Alabama 1975), Contractor shall have the option, in addition to the other remedies of the contract, of renegotiating the Agreement (extending or changing payment terms or amounts) or terminating the Agreement.

14. **Non-Appropriation of Funds.** Pursuant to Section 41-4-144(c) of the Code of Alabama 1975, in the event funds are not appropriated or otherwise made available to support continuation of performance in a subsequent fiscal period, the Agreement may be cancelled and Contractor shall be reimbursed for the reasonable value of any non-recurring costs incurred but not amortized in the price of the services being delivered under the Agreement.

15. **Certification Pursuant to Act No. 2006-557.** Section 41-4-142 of the Code of Alabama 1975 (Act No. 2006-557) provides that every bid submitted and contract executed shall contain a certification that the supplier and all of its affiliates that make sales for delivery into Alabama or leases for use in Alabama are registered, collecting, and remitting Alabama state and local sales, use, and/or lease tax on all taxable sales and leases into Alabama. Contractor hereby certifies it is in full compliance with Section 41-4-142 and acknowledges RSA may declare this Agreement void if the certification is false.

16. **Open Records Law Compliance.** Contractor acknowledges and agrees that RSA may be subject to Alabama open records laws or similar state and/or federal laws relating to disclosure of public records and may be required, upon request, to disclose certain records and information covered by and not exempted from such laws. Contractor acknowledges and agrees that RSA may comply with these laws without violating any provision of Contractor's proposal or this final agreement.

17. **Applicable Law.** This Agreement shall be governed and construed in accordance with Alabama law, without giving any effect to the conflict of laws provision thereof.

18. **Termination.**

Termination for Convenience. This Agreement may be terminated for any reason by either party with the submission of a thirty day written notice of intent thereof.

Termination for Default. RSA may terminate immediately all or any part of this Agreement by giving notice of default by Contractor if the Contractor (1) refuses or fails to deliver the goods or services within the time specified, (2) fails to comply with any of the provisions of the Agreement or so fails to make progress as to endanger or hinder performance, (3) becomes insolvent or subject to proceedings under any law relating to bankruptcy, insolvency, or relief of debtors. In the event of termination for default, RSA's liability will be limited to the payment for goods and/or services delivered and accepted as of the date of termination.

19. **Waiver.** The failure of RSA to require performance of any provision of this Agreement shall not affect RSA's right to require performance at any time thereafter, nor shall a waiver of any breach or default constitute a waiver of any subsequent breach of default nor constitute a waiver of the provision itself.

20. **Entire Agreement.** It is understood by the parties that this instrument, including its exhibit(s), contains the entire agreement of the parties with respect to the matters contained herein (provided, however, that Contractor's Proposal, and the attachments thereto (including without limitation Contractor's best and final offer and Business Associate Agreement, if applicable) shall be incorporated herein for all practical purposes and further provided that to the extent there exists a direct conflict between this Agreement and any of the foregoing, this Agreement shall supersede as to the conflicting provision(s)).

In Witness Whereof, the parties have executed this Agreement effective as of the date first provided above.

Contractor's EIN

Contractor:

By: _____
Its: _____
Date: _____

Retirement Systems of Alabama

By: David G. Bronner
Its: _____
Date: _____

Reviewed and Approved as to Form:

_____

RSA Legal

Approved:

_____

Kay Ivey
Governor, State of Alabama

Exhibit A
Consideration

RSA shall pay to Contractor the following fees for any such services rendered at RSA's request in accordance with the terms more specifically set forth in the Agreement:

™

PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN

Business Associate Policy

December 8, 2015

The Public Education Employees' Health Insurance Plan ("PEEHIP") protects the privacy of personal information in accordance with applicable privacy laws. PEEHIP is required by law to take reasonable steps to ensure the privacy of our members' healthcare information in accordance with the Health Insurance Portability and Accountability Act (**HIPAA**). With the addition of the Health Information Technology for Economic and Clinical Health (**HITECH**) Act, (enacted as part of the American Recovery and Reinvestment Act of 2009), and the final set of rules included in the HIPAA Omnibus rule set in 2013, it is imperative that PEEHIP maintain reasonable oversight over protected health information that it shares with its business associates. As defined by HIPAA, a "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

Policy:

PEEHIP shall ensure that all of its business associate agreements (BAA's) meet current regulation requirements and are reviewed annually by internal staff or others. Any addendum(s) to a BAA that are required by any current or proposed HIPAA or HITECH statutes or regulations shall be entered into within the time frame mandated pursuant to such statutes or regulations.

As a continued or future business associate of PEEHIP, business associates must provide adequate documentation stating they are in compliance with current HIPAA Security and Privacy rules. Documentation must consist of, at a minimum, one of the following:

- **External HIPAA Attestation Report**

  A HIPAA attestation report must be conducted by a credible third party audit firm specializing in HIPAA Privacy and Security audits within the last year. Assessments must continue to be scheduled on a regular yearly basis covering at minimum the last 12 consecutive months of the previous year and not a point in time. The assessment must provide a qualified opinion of whether the business associate meets current HIPAA and HITECH Security and Privacy requirements based on an agreed-upon set of procedures (AUP). Report must be signed by a certified CISA, CISSP, or HCISPP auditor.

- **Service Organization Control Reporting**

  Service Organization Control reports are required by business associates based upon service(s) performed on behalf of PEEHIP. Business associates classified as having a material impact on PEEHIP's financial statement will be required to obtain a **SOC 1 Type 2** report as deemed necessary by PEEHIP. Organizations which provide services to PEEHIP with direct access to public health information (PHI) will be required to complete a **SOC 2 Type 2** relevant to the service(s) being performed by the business associate. A **SOC 2 Type 2** report is required for each trust service principle that is relevant to the outsourced service being performed by the business associate. In most cases PEEHIP will require each business associate to audit their controls against all five trust services principles including: **security**, **privacy**, **availability**, **confidentiality**,

and **processing integrity**. The SOC 2 Type 2 report must be performed directly on the business associate covering the last 12 consecutive months.

If the business associate utilizes or will utilize a managed data service provider or "subservice" such as Amazon or Microsoft Azure Cloud Services, the business associate will be required to produce a separate **SOC 2 Type 2** report based upon contracted service type(s). This report must also cover the last 12 consecutive months without gap.

- Note: For "subservice" providers, a **SOC 2 Type 2** report must include at minimum the following trust services principles: **security**, **availability**, and **confidentiality**. If the "subservice" provider also performs data processing functions for the business associate, the remaining trust service principles, **processing integrity** and **privacy,** will be required as part of the **SOC 2 Type 2** report.

- **HITRUST Certification**
  The HITRUST Common Security Framework (CSF) is a comprehensive and certifiable security framework used by healthcare organizations and their business associates to efficiently approach regulatory compliance and risk management. A current HITRUST certification issued within the last year will be accepted by PEEHIP to meet compliance with this policy.

Policy Enforcement:

If any current or future business associate plans to obtain one of the reports or certifications noted above but currently does not possess it, PEEHIP will accept the following:

- For current business associates, a proof of engagement letter stating they will complete and provide one of the acceptable reports or certifications to PEEHIP within 12 months.
- For new business associates, a proof of engagement letter stating they will complete and provide one of the acceptable reports or certifications to PEEHIP within 90 days of executing the contract.

Initial reports must incorporate more than 90 days' worth of data for testing, while subsequent reports must include the last 12 months of controls testing without gap. If a current business associate fails to comply with this Policy, PEEHIP shall have the right, at PEEHIP's sole discretion, to request one of the above defined audits to be completed and results obtained within a period of time defined by PEEHIP from the date such business associate receives written notice of noncompliance from PEEHIP**. In such event, the audited party will be solely responsible for all expenses incurred by the parties during the audit, including without limitation, all payment due to the audit firm. Should such business associate not agree to an audit within 90 days of receiving written notice of noncompliance from PEEHIP, PEEHIP shall have the right, in its sole discretion, to terminate its relationship with the business associate and/or to impose any such other penalties as PEEHIP may have the right to impose pursuant to the applicable contract and governing law.**

HIPAA Compliance Questions

1. Is everyone in the organization provided HIPAA training? If so, how often?

2. What is the size of the staff within the organization? Is there a defined security and privacy officer? If so, do they have appropriate backgrounds to act within their roles?

3. Please explain how HIPAA assessments are performed within the organization. How often are assessments done, and by whom? May PEEHIP obtain a copy of the latest assessment?

4. If the organization has ever had a HIPAA breach, when did it occur?

5. May PEEHIP obtain a copy of your Information Security Policy and Procedures?

6. At any point in time, may PEEHIP come on site and perform a self- assessment based on HIPAA requirements?

7. Has everyone in the organization been trained on how to report a security incident or potential breach?

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made and entered into this ____ day of _____20__, by and between _____ ("Business Associate") and the Public Education Employees' Health Insurance Board ("Plan Sponsor"), acting on behalf of the Public Education Employees' Health Insurance Plan ("Covered Entity").

WHEREAS, Business Associate and Covered Entity desire and are committed to complying with all relevant federal and state laws with respect to the confidentiality and security of Protected Health Information (PHI), including, but not limited to, the federal Health Insurance Portability and Accountability Act of 1996, and accompanying regulations, as amended from time to time (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and any regulations promulgated thereunder.

NOW, THEREFORE, for valuable consideration the receipt of which is hereby acknowledged and intending to establish a business associate relationship under 45 CFR §164, the parties hereby agree as follows:

I. Definitions

A. "Business Associate" shall have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [**Insert Name of Business Associate**].

B. "Breach" shall be defined as set out in 45 CFR §164.402.

C. "CFR" means the Code of Federal Regulations. A reference to a CFR section means that section as amended from time to time; provided that if future amendments change the designation of a section referred to herein, or transfer a substantive regulatory provision referred to herein to a different section, the section references herein shall be deemed to be amended accordingly.

D. "Compliance Date(s)" shall mean the date(s) established by the Secretary or the United States Congress as the effective date(s) of applicability and enforceability of the Privacy Rule, Security Rule and HITECH Standards.

E. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR §164.501 and shall include a group of records that is: (i) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for Covered Entity by Business Associate or (2) used, in whole or in part, by or for Covered Entity to make decisions about Individuals.

F. "Electronic Protected Health Information" (EPHI) shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.

G. "HITECH Standards" shall mean the privacy, security and security breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, as such law may be amended from time to time, and any regulations promulgated thereunder.

H. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

I. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.

J. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.

K. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR §164.501.

L. "Security Incident" shall have the same meanings as the term "security incident" in 45 CFR §164.304.

M. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR parts 160 and 164, subparts A and C.

N. "Unsecured PHI" shall have the same meaning as "unsecured protected health information" in 45 CFR §164.402.

Terms used, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule, Security Rule and HITECH Standards.

II. Obligations of Business Associate

A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will take reasonable efforts to limit requests for, use and disclosure of PHI to the minimum necessary to accomplish the intended request, use or disclosure and comply with 45 CFR 164.502(b) and 514(d) .

B. To the extent the Business Associate conducts a "Standard Transaction" as outlined in 45 CFR Part 162, Business Associate agrees to comply and to require any agent or subcontractor to comply with all applicable requirements set forth in 45 CFR Part 162.

C. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.

D. Business Associate agrees to report to Covered Entity any use or disclosure of PHI other than as provided for by this Agreement promptly after Business Associate has actual knowledge of such use or disclosure, and to report promptly to the Covered Entity all Security Incidents of which it becomes aware. Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of such Breach without

unreasonable delay, and in no event later than 30 calendar days after such discovery. The notification will include the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during the Breach. A Breach shall be treated as discovered as of the first day on which such Breach is known or reasonably should have been known to Business Associate. The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity is required by applicable laws or regulations. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI, and so long as additional notice to Covered Entity is not required by applicable laws or regulations.

E. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable regulations. Business Associate has a duty to assist the Covered Entity in any mitigation, notice, reporting, or other remedial actions required, all of which would be at the Covered Entity's request and in the Covered Entity's sole discretion.

F. Business Associate agrees to include in its agreement with any agent or subcontractor to whom it provides PHI on behalf of the Covered Entity conditions with respect to such information that are at least as restrictive as those that apply through this Agreement to Business Associate. Business Associate agrees to ensure that any agents, including sub-agents, to whom it provides EPHI received from, or created or received by Business Associate on behalf of the Covered Entity, agree in writing to implement the same reasonable and appropriate safeguards that apply to Business Associate to protect the Covered Entity's EPHI.

G. If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make available to Covered Entity, within a reasonable time, such information as Covered Entity may require to fulfill Covered Entity's obligations to respond to a request for access to PHI as provided under 45 CFR §164.524 or to respond to a request to amend PHI as required under 45 CFR §164.526. Business Associate shall refer to Covered Entity all such requests that Business Associate may receive from Individuals. If Covered Entity requests Business Associate to amend PHI in Business Associate's possession in order to comply with 45 CFR §164.526, Business Associate shall effectuate such amendments no later than the date they are required to be made by 45 CFR §164.526; provided that if Business Associate receives such a request from Covered Entity less than ten (10) business days prior to such date, Business Associate will effectuate such amendments as soon as is reasonably practicable.

H. If applicable, Business Associate agrees to provide to Covered Entity within a reasonable time such information necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures as provided under 45 CFR §164.528. Business Associate shall refer to Covered Entity all such requests which Business Associate may receive from Individuals.

I. Upon reasonable notice, Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the U.S. Secretary of Health and Human Services, or an officer or employee of that Department to whom relevant authority has been delegated, at Covered Entity's expense in a reasonable time and manner, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

J. Notwithstanding any other provision in this Agreement, Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate will comply with the HITECH Business Associate provisions and with the obligations of a Business Associate as prescribed by HIPAA and the HITECH Act commencing on the Compliance Date of each such provision. Business Associate and the Covered Entity further agree that the provisions of HIPAA and the HITECH Act that apply to Business Associates and that are required to be incorporated by reference in a Business Associate Agreement are incorporated into this Agreement between Business Associate and Covered Entity as if set forth in this Agreement in their entirety and are effective as of the Compliance Date.

III. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may:

A. Use or disclose Protected Health Information on behalf of the Covered Entity, if such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary standard, if done by the Covered Entity.

B. Use or disclose PHI to perform the services outlined in the **<applicable services agreement>.**

C. Use Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate.

D. Disclose Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate, provided that such disclosure is either Required by Law or Business Associate obtains reasonable assurances from any person to whom Protected Health Information is disclosed that such person will: (i) keep such information confidential, (ii) use or further disclose such information only for the purpose for which it was disclosed to such person or as Required by Law, and (iii) notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

E. Use Protected Health Information to provide data aggregation services relating to the health care operations of the Covered Entity, as provided in 45 CFR §164.501.

F. To create de-identified data, provided that the Business Associate de-identifies the information in accordance with the Privacy Rule. De-identified information does not constitute PHI and is not subject to the terms and conditions of this Agreement.

G. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

H. Business Associate agrees to ensure that access to EPHI related to the Covered entity is limited to those workforce members who require such access because of their role or function. Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such EPHI from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule

IV. Obligations of Covered Entity

A. Covered Entity shall notify Business Associate of any facts or circumstances that affect Business Associate's use or disclosure of PHI. Such facts and circumstances include, but are not limited to: (i) any limitation or change in Covered Entity's notice of privacy practices, (ii) any changes in, or withdrawal of, an authorization provided to Covered Entity by an Individual pursuant to 45 CFR §164.508; and (iii) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522.

B. Covered Entity warrants that it will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or is not otherwise authorized or permitted under this Agreement.

C. Covered Entity acknowledges and agrees that the Privacy Rules allow the Covered Entity to permit Business Associate to disclose or provide access to PHI, other than Summary Health Information, to the Plan Sponsor only after the Plan Sponsor has amended its plan documents to provide for the permitted and required uses and disclosures of PHI and to require the Plan Sponsor to provide a certification to the Plan that certain required provisions have been incorporated into the Plan documents before the Plan may disclose, either directly or through a Business Associate, any PHI to the Plan Sponsor. Covered Entity hereby warrants and represents that Plan documents have been so amended and that the Plan has received such certification from the Plan Sponsor.

D. Covered Entity agrees that it will have entered into Business Associate Agreements with any third parties to whom Covered Entity directs and authorizes Business Associate to disclose PHI.

V. Effective Date; Termination

A. The effective date of this Agreement shall be the date this Agreement is signed by both parties (or the Compliance Date, if later).

B. This Agreement shall terminate on the date Business Associates ceases to be obligated to perform the functions, activities, and services described in Article III.

C. Upon Covered Entity's knowledge of a material breach or violation of this Agreement by Business Associate, Covered Entity shall notify Business Associate of such breach or violation and Business Associate shall have thirty (30) days to cure the breach or end the violation. In the event Business Associate does not cure the breach or end the violation, Covered Entity shall have the right to immediately terminate this Agreement and any underlying services agreement if feasible.

D. Upon termination of this Agreement, Business Associate will return to Covered Entity, or if return is not feasible, destroy, any and all PHI that it created or received on behalf of Covered Entity and retain no copies thereof. If the return or destruction of the PHI is determined by Business Associate not to be feasible, Business Associate shall limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. If return or destruction of the PHI is feasible but Business Associate is required by law to retain such information or copies thereof, Business Associate will maintain the PHI for the period of time required under applicable law after which time Business Associate shall return or destroy the PHI.

E. Business Associate's obligations under Sections II and III of this Agreement shall survive the termination of this Agreement with respect to any PHI so long as it remains in the possession of Business Associate.

VI. Other Provisions

A. The parties acknowledge that the foregoing provisions are designed to comply with the mandates of the Privacy and Security Rules and the HITECH Standards and agree to make any necessary changes to this agreement that may be required by any amendment to the final regulations promulgated by the Secretary If the parties are unable to reach agreement regarding an amendment within thirty (30 days) of the date that Business Associate receives any written objection from Covered Entity, either party may terminate this Agreement upon ninety (90) days written notice to the other party. Any other amendment to the Agreement unrelated to compliance with applicable law and regulations shall be effective only upon execution of a written agreement between the parties.

B. Except as it relates to the use, security and disclosure of PHI and electronic transactions, this Agreement is not intended to change the terms and conditions of, or the rights and obligations of the parties under any other services agreement between them.

C. Business Associate agrees to defend, indemnify and hold harmless Covered Entity, its affiliates and each of their respective directors, officers, employees, agents or assigns from and against any and all actions, causes of action, claims, suits and demands whatsoever, and from all damages, liabilities, costs, charges, debts, fines, government investigations, proceedings, and expenses whatsoever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims), which may be asserted or for which they may now or hereafter become subject arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of Business Associate under this Agreement; and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with Business Associate's performance under this Agreement.

D. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

E. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity to comply with the Privacy and Security Rules and the HITECH Standards.

F. If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable

G. This Agreement replaces and supersedes in its (their) entirety any prior Business Associate Agreement(s) between the parties.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, this Agreement has been signed and delivered as of the date first set forth above.

Public Education Employees' Health Insurance Board **the Plan Sponsor, acting on behalf of Covered Entity**	**<insert name of Business Associate>**
_____	_____
Signature	*Signature*
_____	_____
Printed Name	*Printed Name*
_____	_____
Title	*Title*