

REQUEST FOR PROPOSALS

FOR

HEALTH INSURANCE COMPLIANCE CONSULTING
(HIPAA and HITECH)

FOR

THE

PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN

For the Fiscal Years

2027 through 2031

October 1, 2026 through September 30, 2031

RFP 26-004

Issue Date: April 17, 2026

THIS RFP CONTAINS INFORMATION UNDER THE FOLLOWING HEADINGS:

SECTION I

General Information for the Proposer

- A. Purpose
- B. Background
- C. Description of PEEHIP's Management
- D. Operations
- E. Other Information
- F. Proposal Opening
- G. Key Dates
- H. Scope of Services
- I. Payment Schedule
- J. Selection of Firm
- K. Economy of Preparation
- L. News Releases
- M. Addenda to the RFP
- N. Contact Point
- O. Minimum Qualifications
- P. Agents
- Q. STAARS Registration
- R. Exceptions

SECTION II

Information Required from Proposers

- A. Qualifications of the Firm
- B. Cost Proposal

SECTION III

Criteria for Evaluation

- A. General
- B. PEEHIP's Rights
- C. Termination
- D. Proposal Evaluation
- E. 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 PEEHIP State Contract
- C. Immigration Compliance Certificate
- D. Proposer Profile Form
- E. Proposer References Form
- F. PEEHIP Statement on HIPAA Compliance Documentation
- G. Sample Business Associate Agreement
- H. IRS Form W-9
- I. Non-Disclosure Agreement
- J. IT Security Questionnaire
- K. Certification of Bidder or Proposer

SECTION I

General Information for the Bidder

A. Purpose:

This Request For Proposal (RFP) solicits vendor proposals to provide audit, training, and consulting services for the Public Education Employees' Health Insurance Board, acting on behalf of the Public Education Employees' Health Insurance Plan (PEEHIP) to ensure PEEHIP's compliance with the Health Insurance and Portability Accountability Act of 1996 and accompanying regulations, as amended from time to time, (HIPAA) and the Health Information Technology for Economic and the Clinical Health Act of 2009 and any regulations promulgated thereunder (HITECH).

B. Background:

The PEEHIP provides hospital medical health insurance benefits for all full-time employees and certain part-time employees of the Alabama public educational institutions, which provide instruction at any combination of grades K-14. These insurance benefits are also available to retired employees with a portion of the retiree's cost paid through the employer premium for active employees. Coverage is also offered to eligible dependents.

Members have the following choices for health insurance coverage as follows:

- Hospital medical administered by Blue Cross and Blue Shield of Alabama – Actives and Non-Medicare eligible retirees and eligible dependents.
- Prescription Drug coverage administered by Express Scripts – Actives and Non-Medicare eligible retirees and eligible dependents.
- Health Maintenance Organization – Viva – Actives and Non-Medicare eligible retirees.
- Medicare Advantage Prescription Drug Plan (MAPDP) – Humana – Medicare eligible retirees and Medicare eligible dependents of retirees
- Optional Coverage administered by Southland Benefit Solutions, LLC – consisting of Dental, Hospital Indemnity, Vision, and Cancer.
- Supplemental Hospital Medical administered by Blue Cross and Blue Shield of Alabama—supplemental coverage for Actives and Non-Medicare eligible retirees

Members electing one of the hospital medical plans must pay a small amount each month for single coverage plus an additional amount if the member elects family coverage. Additionally, members may select the optional coverage plans or supplemental plan in lieu of the hospital medical coverage. Members electing hospital medical coverage may also elect to pay an additional amount to acquire one or more of the optional plans.

C. Description of PEEHIP's Management:

The PEEHIP's self-insurance plan and administrative responsibility for this fund is with the Retirement Systems of Alabama (RSA) administrative staff. The Chief Executive Officer (CEO) of the Teachers' Retirement System (TRS) also serves as CEO for the PEEHIP. All matters relating to the PEEHIP have been assigned to staff who serve under the direction of the Deputy Director for Administration.

D. Operations:

The Accounting Division of the RSA is responsible for budgeting projected claims and working with the insurance consultant to estimate premium rates necessary to fund the claims and maintain adequate reserves for unreported and unpaid claims.

The PEEHIP Division maintains insurance records for the approximately 360,000 active and retired members and eligible dependents via Member Online Services. All changes are reported to the third-party administrators via electronic file transfer.

In March 2007, the Alabama Retired Education Employees' Health Care Trust, a multiple-employer cost-sharing defined benefit post-employment healthcare plan, was established to provide healthcare benefits to retirees of state and local educational institutions. As of September 30, 2025, the assets totaled \$2.7 billion.

Claims paid by third party administrators and payments to HMOs for Fiscal Years 2023-2025 are summarized as follows (cash basis):

(Amount in Millions)

TPA	2023	2024	2025
Medical - BCBS of AL	\$ 1,013	\$ 1,043	\$ 1,119
Drug - ESI	\$ 254	\$ 288	\$ 247
MAPDP	\$ 77	\$ 57	\$ 203
HMO - VIVA	\$ 20	\$ 18	\$ 19
Optionals - CDIV - Southland	\$ 63	\$ 60	\$ 66
Flex	\$ 8	\$ 9	\$ 10
Other (e.g., ADPH)	\$ 5	\$ 6	\$ 5
Total Claims	\$ 1,440	\$ 1,481	\$ 1,669

Number of Members with medical contracts and number of dependents enrolled in PEEHIP Medical Coverage and Optional Coverage as of January 31, 2026:

As of January 31, 2026	Active		Retired		Total		Total Contracts	Covered Persons
	Single	Family	Single	Family	Single	Family		
Hospital/Medical								
Hosp/Med	35,297	52,286	3,753	5,580	39,050	57,866	96,916	230,639
Supplemental	188	1,537	546	770	734	2,307	3,041	8,596
Total Hosp/Med	35,485	53,823	4,299	6,350	39,784	60,173	99,957	239,235
Humana	-	-	40,442	20,437	40,442	20,437	60,879	80,907
Viva Health	727	518	133	90	860	608	1,468	2,747
Total Hospital/Medical	36,212	54,341	44,874	26,877	81,086	81,218	162,304	322,889

As of January 31, 2026	Active		Retired		Total		Total Contracts	Covered Persons
	Single	Family	Single	Family	Single	Family		
Optional Plans								
Cancer	3,850	6,175	4,636	5,127	8,486	11,302	19,788	39,054
Dental	24,340	45,564	28,777	30,718	53,117	76,282	129,399	272,384
Vision	8,585	13,678	7,071	9,488	15,656	23,166	38,822	81,865
Indemnity	2,608	3,825	2,503	2,249	5,111	6,074	11,185	22,141
All optional plans are with Southland								

PEEHIP also implemented a MAPDP effective January 1, 2017. The member count for this program is approximately 81,000 (included above), and the plan is currently administered by Humana.

E. Other Information:

Additional terms and conditions applicable to, and hereby incorporated within, this RFP and all proposals submitted in response to this RFP are located at <https://www.rsa-al.gov/about-rsa/itb-rfp/> and titled:

- RSA Reservation of Rights and Requirements for ITBs and RFPs
- RSA Standard Terms and Conditions for Solicitations and Contracts
- RSA Procedure for Resolution of Controversies

By submitting a proposal, all proposers are 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 therefore.

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

RSA's website – www.rsa-al.gov

PEEHIP information on RSA's website – www.rsa-al.gov/index.php/members/peehip/

Alabama Secretary of State's website – www.sos.alabama.gov

PEEHIP Law – *Code of Alabama 1975, Title 16, Chapter 25A, Article 1*

Flexible Benefits Plan Law – *Code of Alabama (1975), Title 16, Chapter 25A, Article 2*

F. Proposal Opening:

Please submit one printed non-redacted and one printed redacted copy of your proposal, and a digital copy (non-redacted and redacted) on a USB drive in a sealed envelope with the following plainly marked on the front:

PEEHIP
HEALTH INSURANCE COMPLIANCE CONSULTING PROPOSAL
RFP 2026-004
OPENING June 4, 2026

Proposals will be sent to:

Proposals sent via UPS or FedEx:

Taylor Benefield
Accounting Dept.
Retirement Systems of Alabama
201 South Union Street
Montgomery, AL 36104

Proposals sent via U.S. Mail:

Taylor Benefield
Accounting Dept.
Retirement Systems of Alabama
P.O. Box 302150
Montgomery, AL 36130-2150

Proposals may be hand delivered to Taylor Benefield of the Retirement Systems Building, 7th floor, 201 South Union Street, Montgomery, Alabama. Proposals will be accepted until 2:00 p.m. CST on June 4, 2026. Proposals will not be accepted after this date and time. Proposals will be opened after 2:00 p.m. CST on June 4, 2026. PEEHIP reserves the right to reject any and all responses to this RFP.

Any questions regarding this RFP must be submitted electronically via email by May 1, 2026, at 2:00 p.m. CST to Taylor Benefield at Taylor.Benefield@rsa-al.gov.

All responses to this solicitation may be subject to public disclosure upon request. Proposers should be aware of the Open Records Act (Ala. Code §36-12-40), the Alabama Trade Secrets Act (Ala. Code §8-27-1 and §8-27-6), and the Public Record Status of Certain Procurement Information statute (Ala. Code §41-4-115).

Any confidential, trade secret, or proprietary commercial information contained in a proposal must be clearly marked as such. Identification of an entire proposal as confidential is not acceptable unless the proposer states in detail the specific grounds and applicable laws which support treatment of the entire proposal as protected from disclosure.

G. Key Dates:

RFP 26-004 KEY DATES	
Activity	Date
RFP to be Issued/Posted on RSA's website	April 17, 2026
Deadline to Submit Questions	May 1, 2026 @ 2:00 p.m. CST
Responses to Questions posted to RSA's website	May 6, 2026 @ 5:00 p.m. CST
Responses Due by	June 4, 2026 @ 2:00 p.m. CST
Bid Opening Date	June 4, 2026
Finalist Conferences (if held)	Week of June 8, 2026
Award of Bid	June 12, 2026

H. Scope of Services:

Compliance requirements for HIPAA, HITECH, and Healthcare Reform are constantly evolving. PEEHIP is required to stay abreast of those changes in order to appropriately safeguard protected health information (PHI) and reduce adverse impacts to the fund. The requirements listed below will help PEEHIP ensure the plan stays consistent with meeting those objectives and become further proactive in fulfilling the requirements issued by Health and Human Services (HHS). PEEHIP requires all compliance and training materials to be updated at minimum on a yearly basis or more frequently as required by legislation.

Specific services required include:

- Providing highly qualified legal guidance to the PEEHIP management team regarding legal/legislative developments related to healthcare security, privacy, and confidentiality. PEEHIP requires legal opinions to be issued by personnel with an official Juris Doctor degree and a subject matter expert in the area of healthcare security and privacy. A team of HIPAA experts should be assigned to PEEHIP in the event of an emergency by providing a call tree and escalation plan for after-hours emergencies.
- Providing yearly in-person compliance training (or, at PEEHIP's sole discretion, computer-based live or recorded training) to all PEEHIP staff with updated training materials reflecting new or modified legislation and regulatory guidance, which also includes performing a gap analysis of training content. Training materials and in-person training should be completed by successful proposer no later than February 28 of each contract year. In the event that training cannot be performed onsite due to a national pandemic, or other cause deemed by PEEHIP as prohibiting onsite training, proposer must be able to create content and conduct training remotely. Proposer must be able to capture the training in a format that can be easily replayed by PEEHIP and RSA employees and provide the recording to RSA within thirty (30) days from the in-person training if requested by PEEHIP.
- Reviewing Business Associate Agreements (BAA) to ensure verbiage is updated and complies with health care security and privacy regulations.
- Providing yearly HIPAA/HITECH security and privacy assessments based on established industry frameworks for auditing healthcare plans, with compliance reports completed by June 30th each year.
- Conducting onsite visits to determine if physical security requirements comply with HIPAA privacy and security regulations.
- Updating PEEHIP policy handbooks to reflect changes in regulations and operating procedures.
- Attending PEEHIP board meetings as requested by management to address compliance or litigation concerns that may arise.
- Interviewing select management and staff members regarding common privacy and security-related practices within PEEHIP to include, but not be limited to, disposal, storage, and encryption practices or procedures.
- Identifying all information systems and communication networks that store, maintain, or transmit electronic PHI and determine compliance with documented HIPAA privacy and security regulations or other state privacy and security statutes related to healthcare.
- Evaluating potential risks (to include the cost of failure related to privacy or security breaches and related public communication costs) associated with how PEEHIP collects, uses, manages, houses and discloses

health information and evaluate options or changes to current practices in order to meet HIPAA Privacy and Security regulations or other state privacy and security statutes. Evaluate risks related to current policies, procedures, tools, and techniques related to management investigation and remediation of privacy or security breaches.

- Determining if PEEHIP procedures for release, disclosure and recording of health information comply with each of the HIPAA Privacy and Security standards.
- Determining if breach notification procedures are appropriate, sufficient, and up to date.
- Assisting with any other HIPAA/HITECH consulting requested from time to time by PEEHIP.

I. Payment Schedule:

Payments will be made no more frequently than monthly based upon the firm's actual hours worked. PEEHIP requires payment terms to be payable 30 days from receipt of invoice.

J. Selection of Firm:

PEEHIP reserves the right to make no award under this RFP. PEEHIP expects to enter into a contract with the successful proposer(s). PEEHIP also reserves the right to award all or part of required services under this RFP to one or more proposers, and this decision will be at the sole discretion of PEEHIP. PEEHIP makes no guarantee that the successful proposer(s) will be the exclusive provider(s) of the services during the term of any resulting contract. All firms submitting a proposal under this RFP will be notified in writing within a reasonable length of time following the selection. Prior to an award of contract(s), one or more proposers who submit proposals determined to be reasonably susceptible of being selected for award may be requested to make oral presentations to the evaluation committee; however, proposals may be accepted, and a final selection made, without such oral presentations. All proposals shall become the property of the PEEHIP.

Internet and/or website links will not be accepted in responses as a means to supply any requirements stated within this solicitation. Unless stated elsewhere in this solicitation, PEEHIP will accept and evaluate alternate submittals on this RFP provided that the response meets all published requirements. PEEHIP reserves the right to waive minor discrepancies or errors within proposals or to request clarification from a proposer to the extent allowed by law.

The failure of PEEHIP to require performance of any provision of the solicitation or resulting contract shall not affect PEEHIP'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 or default nor constitute a waiver of the provision itself.

K. Economy of Preparation:

Proposals should be prepared simply and economically and provide a concise description of the bidder's response to the requirements of this RFP. Emphasis should be on clarity. PEEHIP will not be responsible for any costs incurred by any bidder in the preparation of a proposal.

L. News Releases:

News releases pertaining to this RFP, the service, or the audits to which it relates will be made only with prior written approval of the CEO or his representative.

M. Addenda to the RFP:

RSA may, at any time prior to the deadline for proposals, modify this RFP, including the timeline associated with the RFP. Any modifications made to the RFP prior to the proposal's due date will be provided in writing to all solicited vendors.

N. Contact Point:

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

O. Minimum Qualifications:

Proposals will be accepted from firms where both the firm and the assigned lead consultant have consulted with and advised a self-insured health insurance plan on its HIPAA security and privacy practices, with such plan having at least 150,000 covered lives and claims of at least \$500 million annually. This experience should be for three (3) years of the most recent five (5) years. Subcontractors and joint ventures are not approved to bid on this RFP.

The proposer shall affirmatively state and describe how it meets all of the minimum experience requirements as noted in this Section as a part of its response to this RFP.

P. Agents:

No agents' fees will be payable by PEEHIP or successful vendor. PEEHIP will respond only to parties interested in proposing and performing the services.

Q. STAARS Registration:

Successful proposer must be registered and subscribed in the STAARS Vendor Self Service Portal (VSS) at <https://procurement.staars.alabama.gov> prior to contract award and execution of contract.

R. Exceptions.

By signing the proposal, Proposer agrees to be bound by all terms and conditions of the RFP. Any exceptions to the specified terms and conditions must be clearly set forth within Proposer's proposal and are subject to the acceptance of PEEHIP.

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, limited liability company, or corporation, and provide the state in which your company was incorporated or formed. State whether you are licensed to operate in the State of Alabama.

2. Experience:

As part of the proposal, the proposer shall provide a concise narrative (not to exceed ten (10) pages) describing the proposer's understanding of the services requested under this RFP, the qualifications and relevant experience of the personnel who will be assigned to the engagement, and the firm's experience performing similar services for comparable organizations. Marketing materials or general corporate background brochures should not be included.

The narrative should emphasize experience directly applicable to providing HIPAA and HITECH compliance audit, training, and consulting services for health plans, particularly governmental or large self-insured plans. Proposers should also identify a contact person for large self-insured clients for whom similar services have been performed per subparagraph "e" below.

The proposal must address the specific experience and qualifications outlined in the sections below.

a. Understanding of the Engagement

Provide a narrative demonstrating the proposer's understanding of the services requested under this RFP, including:

- The proposer's understanding of PEEHIP's need for HIPAA and HITECH compliance support, including audit, training, and consulting services.
- Key risks, regulatory considerations, and operational issues relevant to health plan compliance with HIPAA and HITECH.

b. Scope and Methodology

Describe the specific services the proposer will provide, including:

- The proposed approach to conducting HIPAA privacy, security, and breach notification compliance reviews.
- Methods for identifying compliance gaps and recommending corrective actions.
- Approach to training PEEHIP staff and Board members regarding HIPAA and HITECH requirements.

c. Personnel Assigned to the Engagement

Identify the personnel who will be assigned to this engagement and provide the following information:

- Name, title, and role of each key individual.
- Relevant professional qualifications and certifications.
- Years of experience performing HIPAA/HITECH compliance services.
- Description of relevant experience with public sector health plans or governmental entities.
- Identification of the individual who will serve as the primary engagement lead and point of contact.

d. Relevant Experience

Provide a description of the proposer's experience performing services similar to those requested in this RFP, including:

- Experience conducting HIPAA and HITECH compliance audits or assessments.
- Experience providing training and consulting services related to HIPAA privacy, security, and breach notification rules.
- Experience working with governmental health plans, large public employers, or health insurance programs.
- Examples of similar engagements completed within the last five years.

e. References

Provide at least three (3) references for organizations for which the proposer has performed similar services. For each reference include:

- Organization name
- Contact person and title
- Telephone number and email address
- Description of services provided
- Covered Lives
- Annual Claims Costs
- Duration of the engagement

3. Authorized Officials:

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

4. Additional Confirmations to be Provided in Proposals:

- a. Confirm whether any consultants or management personnel in your firm who will be providing services to PEEHIP have been censured or fined by any judicial, governmental, or regulatory body in the last five years. If so, please explain.
- b. 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. By submitting your proposal, you are hereby certifying that your firm is in full compliance with Section 41-4-142, you are not barred from bidding or proposing or entering into a contract as a result, and you acknowledge that RSA may declare the contract void if this certification is false.
- c. Proposer certifies that it is not currently, nor has it been, in any agreement of collusion among suppliers in restraint of freedom of competition by agreement to propose at any certain fixed price or to refrain from proposing.

B. Cost Proposal:

The information requested in this Section is required to support the reasonableness of your proposal price.

Reflect the details of each of the following you expect for the annual HIPAA/HITECH compliance consulting services for each of the fiscal years 2027 through 2031.

- Cost per hour for the lead consultant who will be responsible for consulting with PEEHIP and the cost per hour of any other professional person by name and title who will be assisting the lead consultant in performing these consulting services. Include expected number of hours for each proposed person for each year of the contract. Please use the following format:

Fiscal Year 20##			
Professional Name	Role	Cost Per Hour	Expected Number of Hours
		\$	#
		\$	#
		\$	#
Totals		\$	#

- PEEHIP prefers that any incidental fees be included within the hourly rates of the consultants. In the event that is not possible, please include a detailed list of any costs or fees that Proposer expects to be billed to PEEHIP during the contract outside of consultant hourly rates. These should include any travel related expenses. Include a detail basis for charging travel costs or other fees related to the performing of these services. Please note that PEEHIP will only pay travel based upon State of Alabama rules and regulations. Further, PEEHIP will not pay to the contracted vendor any category of expenses or fees not disclosed as part of a cost proposal hereunder.
- Expected total contract cost by year for fiscal years 2027, 2028, 2029, 2030 and 2031 for the services detailed in Section I.H of this RFP.

SECTION III

Criteria for Evaluation

A. General:

The following process will be used to evaluate vendor proposals:

1. A review committee will evaluate each proposal submitted in response to these Proposal specifications.
2. 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.
3. Each proposal will be reviewed and points awarded to all items indicated on the Proposal Evaluation Form. Any proposal component may be awarded points not to exceed the maximum specified on the Proposal Evaluation Form. The total technical score available is 70 points.
4. Each proposal component will be summed to obtain a total score.

B. PEEHIP's Rights

Proposers should note that PEEHIP reserves the right to modify this evaluation structure if it is deemed necessary or request additional information from proposers. It is the intention of PEEHIP to select the most qualified and cost-effective proposal(s) based on the evaluation of the Proposer's responses to this RFP. However, PEEHIP reserves the right to ask vendors for additional information and/or an oral presentation to clarify their proposals. PEEHIP also reserves the right to cancel or terminate the RFP or reject any or all proposals received in response to this RFP.

C. Termination

PEEHIP reserves the right to terminate any resulting contract at any time and at PEEHIP’s discretion by providing a 30-day written notice to the vendor.

D. Proposal Evaluation:

The following factors will be the criteria in making the selection (order does not indicate priority):

1. Description of Services
2. Experience of Personnel Assigned
3. Experience with Similar Proposals
4. IT Security Risk

Cost scoring will be determined as follows:

1. The Proposer submitting the lowest Total Proposal for HIPAA/HITECH compliance consulting services will receive 30 points.
2. All other Proposers will be evaluated by use of the following formula:

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

E. Proposal Evaluation Form

General Proposal Categories	Possible Points	Reviewer’s Score
Description of Services to be Performed	20	
Experience of Personnel Assigned	20	
Experience with Similar Proposals	20	
IT Questionnaire	10	
Total Technical Score	70	
Cost Proposal	30	
Total Possible Points	100	

Finalist Interviews will allow for a possible additional 10 points per proposer offered a finalist interview, at the discretion of the committee, based upon clarifications received from proposer(s) during the discussions.

Proposers must respond to all required components of the RFP.

SECTION IV

Additional Documents

The following documents are referenced in this RFP and must be completed and submitted with the proposal:

- A. State of Alabama Disclosure Statement (Pursuant to the *Code of Alabama 1975, Title 41, Chapter 16, Article 3B*). Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/State_of_Alabama_Disclosure-Statement_Fillable_Form.pdf
- B. Sample PEEHIP 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. Attached to this RFP.
- C. Immigration Compliance Certificate. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/Immigration_Compliance_Certificate.pdf
- D. Proposer Profile Form. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/Proposer_Profile_Form.pdf
- E. Proposer References Form. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/Proposer_References_Form.pdf
- F. PEEHIP Statement on HIPAA Compliance Documentation with Proposer Attestation of Compliance. Attached to this RFP.
- G. 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. Attached to this RFP.
- H. IRS Form W-9. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/IRS_Form_W-9_Fillable_Form.pdf
- I. 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. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/Confidentiality_and_Nondisclosure_Agreement_Form_REV_6_30_2023.pdf
- J. IT Security Questionnaire. Attached to this RFP.
- K. Certification of Bidder or Proposer. Located on the PEEHIP website at https://www.rsa-al.gov/uploads/files/Certification_of_Bidder_or_Proposer.pdf

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 _____, 2026, by and among
The Teachers' Retirement System of Alabama, the Employees' Retirement System of Alabama,
and the Judicial Retirement Fund ("RSA"), and _____, hereinafter referred to
as "Contractor".

RECITALS

- A. RSA issued an RFP for _____ services, and Contractor was awarded this contract based upon the terms of Contractor's Proposal dated _____, 2026 ("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.

3. **Term.** This Agreement shall be for the period beginning _____, 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.
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, commercial general liability insurance, workers compensation insurance, employers’ liability 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 have an A.M. Best Rating of “A-“or better and a financial rating of Class VII or larger. 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 and shall state that this coverage shall be primary insurance for the additional insureds. 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. Free Trade Clause.** In compliance with Ala. Code §41-16-5, 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. Economic Boycott Prohibition.** In compliance with Ala. Code §41-16-161, Contractor hereby certifies that Contractor, without violating controlling law or regulation does not and will not, during the term of this Agreement, engage in economic boycotts.
- 13. 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.

- 14. 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 Ala. Code §41-4-90), 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.

- 15. Non-Appropriation of Funds.** Pursuant to Ala. Code §41-4-144(c), 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.
- 16. Certification Pursuant to Act No. 2006-557.** Ala. Code §41-4-142 provides that every bid submitted, and contract executed, shall contain a certification that the supplier and all 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 §41-4-142 and acknowledges RSA may declare this Agreement void if the certification is false.
- 17. 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.
- 18. 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.
- 19. 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.

- 20. Artificial Intelligence.** Contractor agrees that it will not, under any circumstance, provide RSA information or RSA member data to an Artificial Intelligence (AI) tool without the prior express written consent of RSA following specific disclosure by Contractor of information to be disclosed to AI. Contractor agrees that it will provide prior written notification to RSA regarding any potential AI utilization that may occur in relation to any portion of the services provided hereunder. Contractor further agrees that for any services and/or work product for which AI is utilized, Contractor will indicate in writing to RSA that such services and/or work product involve AI utilization and will further indicate in writing to RSA whether Contractor independently verified the accuracy, validity, and reliability of any and all AI assistance and/or output. Contractor understands and agrees that, in addition to any other indemnification obligation contained in this agreement, Contractor assumes full responsibility and liability regarding Contractor's use of AI in the performance of services and agrees to indemnify and hold harmless RSA related to any errors resulting from the use of AI and/or Contractor's disclosure of confidential or health information to AI.

21. 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.

22. 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:

The Teachers' Retirement System of Alabama, The Employees' Retirement System of Alabama, and the Judicial Retirement Fund, collectively The Retirement Systems of Alabama

By: _____
Its: _____
Date: _____

By: David G. Bronner
Its: Secretary-Treasurer
Date: _____

Reviewed and Approved as to Form:

Approved:

RSA Legal Counsel

Kay Ivey
Governor, State of Alabama



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.**

PEEHIP BUSINESS ASSOCIATE POLICY

1. On behalf of the Bidder or Proposer for this solicitation, I confirm that I have read the PEEHIP Business Associate Policy dated December 8, 2015.
2. Bidder/Proposer is in compliance with current HIPAA Security and Privacy rules, as contemplated under the PEEHIP Business Associate Policy as of the date of this Verification.
3. Bidder/Proposer shall timely submit the following documentation of such compliance (please check all that apply):

- a. External HIPAA Attestation Report
- b. Service Organization Control Report
- c. HITRUST Certification
- d. Proof of Engagement Letter stating Bidder/Proposer will complete and provide one of the acceptable reports or certifications to PEEHIP within 180 days of a signed contract with PEEHIP.

4. I have full authority to represent and bind Bidder/Proposer.

Name of Bidder or Proposer: _____

Dated: _____

Signature: _____

Print Name: _____

Title: _____

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

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
A. Policy			
1	Is there a corporate information security policy in place? If yes, provide as an attachment.		
2	Does the policy state what is and is not permissible as it pertains to sensitive company and customer information?		
3	Does the policy identify what is classified as sensitive company and customer information?		
4	Does the policy identify management and employee responsibilities including contractors?		
5	Does the policy identify use of employee owned devices such as laptops, smart phones, and any other form of device capable of storing data?		
6	Does the policy address change management requirements?		
7	Is there a policy on the portable media?(e.g., thumb drives, CDRW, etc.)		
8	Are personnel and contract personnel required to have national background check performed as part of your security policy? Please provide a copy of Proposers personnel policy if this is separate addressing hiring and termination procedures.		
B. Procedures			
1	Are procedures in place to implement the information security policy?		
2	Are the procedures and standards evaluated to determine their level of impact to the business process?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
3	Does the project management methodology uphold the security practices? If yes, explain how.		
4	Are there policy and procedures in place to vet and audit subcontractors prior to contract acceptance where applicable?		
C. Document Handling			
1	Is there a reasonable and usable information classification policy?		
2	Does the information classification policy address all enterprise information?		
3	Is an information classification methodology in place to assist employees in identifying levels of information within the business unit?		
4	Is there an information handling matrix that explains how specific information resources are to be handled?		
II. Corporate Practices			
A. Organizational Suitability			
1	The Information Security Program has an executive level committee assigned for reporting and guidance purposes?		
2	Are employees able to perform their duties efficiently and effectively while following security procedures?		
3	Does the information security program have its' own line item in the budget?		
4	Does the security group have the authority to submit needed security policy changes throughout the enterprise?		
5	Is an annual report on the level of information security compliance issued to management?		

RSA Third Party Vendor - Security Questionnaire

	Proposer Name:	Date:	
	Prepared By:	Title:	
Factors:			
	I. Security Policy	YES/NO/NA	Comments
6	Is there more than one person responsible for the implementation of the Information Security Program?		
B. Personnel Issues			
1	Are employees able to work less than a 50 hour work week on a monthly average and complete their assignments?		
2	Are employees and project managers aware of their responsibilities for protecting information resources via written policy?		
3	Are technical employees formally trained to perform their tasks?		
4	Are contract personnel subject to confidentiality agreements?		
5	Are contract personnel subject to the same policies employees are?		
6	Is access to sensitive/confidential information by contract personnel monitored?		
7	Are national background checks performed on all proposing party employees?		
8	Is a similar screening process carried out for contractors and temporary staff?		
9	Does employment application ask if the prospective employee has ever been convicted of a crime? If so, does proposing firm employee individuals with felony convictions?		
10	Are prior employment verifications performed for initial employment?		

RSA Third Party Vendor - Security Questionnaire

	Proposer Name:	Date:	
	Prepared By:	Title:	
Factors:			
	I. Security Policy	YES/NO/NA	Comments
11	Are there any current or pending litigations against staff, former staff, or contract staff regarding corporate espionage, identity theft, or any other areas regarding the security of privacy of confidential information?		
C. Training and Education			
1	Do employees receive security related training specific to their responsibilities? If yes, please attach a sample.		
2	Are employees receiving both positive and negative feedback related to security on their performance evaluations?		
3	Is security-related training provided periodically to reflect changes and new methods?		
4	Are system administrators given additional security training specific to their jobs?		
5	Have employees undergone a HIPAA training class for those handling personal health information (PHI)?		
D. Oversight and Auditing			
1	Is Proposer at minimum AICPA SOC 1 Type 2 compliant for financial reporting. If so, please provide the SOC report(s).		
2	Is Proposer's datacenter AICPA SOC 2 Type 2 compliant? If not please comment what compliance level your datacenter facility meets.		
3	Are the security policies and procedures routinely tested?		
4	Are exceptions to security policies and procedures justified and documented?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:

Date:

Prepared By:

Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
5	Are audit logs or other reporting mechanisms in place on all platforms?		
6	Are errors and failures tracked?		
7	When an employee is found to in non-compliance with security policies, has appropriate disciplinary action been taken?		
8	Are audits performed on an annual basis?		
9	Are unscheduled/surprise audits performed?		
10	Has someone been identified as responsible for reconciling audits?		
11	Does either an internal or external auditor independently audit Proposer's operational controls on a periodic basis?		
12	Is an independent review carried out in order to assess the effective implementation of security policies?		
13	Can the Proposer provide evidence of having gone through a recent audit of their organization's operational policies, procedures, and operating effectiveness, such as a SOC Type 2 report?		
14	Have outside audits been performed on internal operations? Please provide copies.		
15	Has Proposer experienced a security breach of corporate or customer data within the last 10 years?		
16	Is there is any concluded or pending litigation against the Proposer or an employee related to a contract engagement or security breach?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
17	Does the Proposer subcontract services that will be required to fulfil services as required in RSA's RFP.		
18	Does Proposer have a change management committee? Does it meet on regularly scheduled intervals?		
E. Application Development and Management			
1	Has an application development methodology been implemented?		
2	Are appropriate/key application users involved with developing and improving application methodology and implementation process?		
3	Is pre-production testing performed in an isolated environment?		
4	Has a promotion to production procedures been implemented?		
5	Is there a legacy application management program?		
6	Are secure coding standards implemented and are they followed?		
7	Are applications testing for security vulnerabilities prior to being released to production?		
8	Is there a dedicated security team for testing applications for vulnerabilities?		
9	Are there procedures in place for protecting source code developed by the Proposer (physically and electronically)?		
10	Is system access and security based on the concept of least possible privilege and need-to-know?		
11	Does Proposer perform source code reviews for each release?		
12	Are backdoors prevented from being placed into application source code?		
III Physical Security			
A. Physical and Facilities			

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
1	Is access to the building(s) controlled?		
2	Is access to computing facilities controlled more so than to the building?		
3	Is there an additional level of control for after-hours access?		
4	Is there an audit log to identify the individual and the time of access that is monitored by a group other than Information Technology?		
5	Are systems and other hardware adequately protected from theft?		
6	Are procedures in place for proper disposal of confidential information?		
7	Are proper fire suppression systems located in the facility?		
8	Are facilities more than 5 miles from a government facility or airport?		
9	Are the servers and facilities that house software documentation and programming logic located in a secure facility?		
10	Is all confidential and restricted information marked as such and stored in a secure area (room, cabinet) with access restricted to authorized personnel only?		
11	Does Proposer allow employees to work remote or in a virtual environment? Please provide documentation around controls for safeguarding computer systems and confidential data.		
B. After-Hours Review			
1	Are areas containing sensitive information properly secured?		
2	Are workstation secured after-hours?		
3	Are keys and access cards properly secured?		
4	Is confidential information properly secured?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
5	Are contract cleaning crews activities monitored?		
	C. Incident Handling		
1	Has an Incident Response Team (IRT) been established?		
2	Have employees been trained as to when the IRT should be notified?		
3	Has the IRT been trained in evidence gathering and handling?		
4	Are incident reports issued to appropriate management?		
5	After an incident, are policies and procedures reviewed to determine if modification need to be implemented?		
6	Does the Proposer have a process in place to notify IT security of breaches and/or problems so that proper notification and correction can be done?		
	D. Contingency Planning		
1	Has a Business Impact Analysis been conducted on all systems, applications, and platforms?		
2	Is there a documented data center Disaster Recovery Plan (DRP) in place?		
3	Are backup media password protected or encrypted?		
4	Has the data center DRP been tested within the past 12 months?		
5	Are system, application, and data backups sent to a secure off-site facility on a regular basis?		
6	Are Service Level Agreements that identify processing requirements in place with all users and service providers?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
7	Have departments, business units, groups, and other such entities implemented business continuity plans that supplement the data center DRP?		
8	Have Emergency Response Procedures (ERP) been implemented?		
9	Have ERPs been tested for effectiveness?		
	IV. Business Impact Analysis, Disaster Recovery Plan		
	A. General Review		
1	Backup planning includes identification of all critical data, programs, documentation, and support items required performing essential task during recovery?		
2	The BIA is reviewed and updated regularly with special attention to new technology, business changes, and migration of applications to alternative platforms?		
3	Critical period timeframes have been identified for all applications and systems?		
4	Senior management has reviewed and approved the prioritized list of critical applications?		
	B. Disaster Recovery Plan (DRP)		
1	A corporate disaster recovery plan coordinator has been named and a mission statement identifying scope and responsibilities has been published?		
2	A "worst-case" scenario DRP to recover normal operations within the prescribed timeframes has been implemented and tested?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
3	Listing of current emergency telephone numbers for police, fire department, medical aid, and company officials are strategically located throughout the facility and at off-site locations?		
4	The backup site is remote from hazards that endanger the main data center?		
5	Contracts for outsourced activities have been amended to include service providers' responsibilities for DRP?		
6	Lead times for communication lines and equipment, specialized devices, power hookups, construction, firewalls, computer configurations, and LAN implementation have been factored into the DRP?		
7	At least one copy of the DRP is stored at the backup site and is updated regularly?		
8	Automatic restart and recovery procedures are in place to restore data files in the event of a processing failure?		
9	Contingency arrangements are in place for hardware, software, communications, software, staff and supplies.		
10	Customer software solutions that are being developed and/or in production are backed up as part of the Proposer's backup and recovery procedures?		
	C. Testing		
1	Backup and recovery procedures are tested at least annually?		
2	Training sessions are conducted for all relevant personnel on backup, recovery, and contingency operating procedures?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
3	Appropriate user representative have a particular role in creating and reviewing control reliability and backup provisions for relevant applications?		
4	Appropriate user representatives participate in the DRP tests?		
	Other Issues		
1	Provisions are in place to maintain the security of processing functions in the event of an emergency?		
2	Insurance coverage for loss of hardware and business impact is in place?		
	V. Technical Safeguards		
	A. Passwords		
1	Are host systems and servers as well as application servers secured with unique passwords?		
2	Are default accounts de-activated?		
3	Are temporary user accounts restricted and disabled within 4 hours?		
4	Are the password management systems forcing users to change passwords every 90 days or less?		
5	Are users of all company-provided network resources required to change the initial default password?		
6	Are the passwords complex? Contain upper case, lower case, special character or number, and at least 8 characters long.		
7	Do network and system administrators have adequate experience to implement security standards?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
8	Are reports and logs pertaining to network users reviewed and reconciled on a regular basis?		
9	Are permissions being set securely?		
10	Are administrators assigned a unique ID for access to critical systems?		
11	Are administrators using appropriate tools to perform their jobs?		
12	Does the application support multi-factor authentication?		
13	Are online systems always secured using SSL encryption?		
	B. Infrastructure		
1	Is the network infrastructure audited on an annual basis?		
2	Are network vulnerability assessments conducted on an annual basis?		
3	Are changes/improvements made in a timely fashion following network vulnerability assessments?		
4	If you house or develop solutions around credit card transactions are you CISP compliant?		
	C. Firewalls		
1	Are protocols allowed to initiate connections from "outside" the firewall?		
2	Has a risk analysis been conducted to determine if the protocols allowed maintain an acceptable level of risk?		
3	Has the firewall been tested to determine if outside penetration is possible?		
4	Are other products in place to augment the firewall level security?		
5	Are the firewalls maintained and monitored 24x7?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
6	Have services offered across the firewall been documented?		
7	Has a Demilitarized Zone (DMZ) or Perimeter Network been implemented?		
8	Has the firewall administrator been formally trained?		
9	Is there more than one person administering the firewall?		
10	Is the firewall for the ASP separate from the corporate firewall?		
	D. Data Communications		
1	Is there a remote access procedure in place?		
2	Is there a current network diagram?		
3	Are Access Control List (ACLs) maintained on a regular basis?		
4	Is the network environment partitioned?		
5	Are the corporate routers separated from the ASP routers?		
6	Are the corporate switches separated from the ASP switches?		
7	Does the communication equipment log administrative access to the systems?		
8	Is SNMP data collected from the data communication devices?		
9	Is syslog data collected from the data communication devices?		
10	Are there standard templates for configuring routers?		
11	Are there standard templates for configuring switches?		
	E. Databases		
1	Are default database passwords changed?		
2	Are database administrators trained or certified?		
3	Are database backups performed daily?		
	F. Computing Platforms		
1	Are critical servers protected with appropriate access controls?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
2	Are development staff administrators on their computers used for writing source code?		
3	Is there a company image used for corporate PCs and laptops?		
4	Does the company have an asset management system to track software installed?		
5	Is there an anti-virus application installed on all PC's, laptops, and servers?		
6	Does the anti-virus application automatically update computing assets 3 times or more per day?		
7	Is there a URL filtering solution in place?		
8	Do computing assets have a corporate anti-malware application installed?		
9	Are Internet facing servers protected with host based intrusion prevention?		
10	Are employees restricted to what can be installed on their computer systems? How is this managed for remote employees if applicable?		
11	Do any of the Proposer's computer systems including storage reside on a cloud computing environment? Is it owned and operated by the Proposer? If no, please explain.		
G. Intrusion Prevention			
1	Is host based intrusion prevention software installed on all Internet facing servers?		
2	Are network based intrusion prevention systems in-line and defending?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
3	Is host based intrusion prevention software installed on all laptops?		
4	Is there a dedicated security staff monitoring 24x7 alerts from the host based intrusion prevention?		
5	Is there a dedicated security staff monitoring 24x7 alerts from the network based intrusion prevention?		
VI. Telecommunications Security			
A. Policy			
1	Is there a published policy on the use of organizational telecommunications resources?		
2	Have all employees have been made aware of the telecommunications policy?		
3	Employees authorized for Internet access are made aware of the organization's proprietary information and what they can discuss in open forums?		
4	Employees using cellular or wireless phones are briefed on the lack of privacy of conversations when using unsecured versions of technology?		
5	The organization has a published policy on prosecution of employees and outsiders if found guilty of serious premeditated criminal acts against the organization?		
6	Are corporate devices such as iPhones or Android based phones centrally managed by the Proposer to control rogue software installations and protect corporate data?		
B. Standards			

RSA Third Party Vendor - Security Questionnaire

Proposer Name:	Date:
Prepared By:	Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
1	A threshold is established to monitor and suspend repeated unsuccessful dial-in or remote access attempts?		
2	Access to databases reachable via dial-in or VPN have access control in place to prevent unauthorized access?		
3	Financial applications available via dial-in or VPN have audit trails established to track access and transaction usage?		
4	Are audit trails reviewed and corrective action taken on a regular basis?		
5	When possible are all security programs used to control dial-in or remote access to a specific application?		
6	Company proprietary data, stored on portable computers are secured from unauthorized access?		
7	Are corporate emails allowed to be sent from unique domains not one used by Proposer such as Gmail or Microsoft Email?		
8	Users of all company-provided communication systems are required to change the default or initial password?		
	C. Practices		
1	Security, application, and network personnel actively work to ensure control inconvenience is as minimal as possible?		
2	Personnel independent of the operations staff and security administration review tamper-resistant logs and audit trails?		
3	Special procedures and audited user IDs have been established for application, system, network troubleshooting activities?		

RSA Third Party Vendor - Security Questionnaire

Proposer Name:

Date:

Prepared By:

Title:

Factors:

	I. Security Policy	YES/NO/NA	Comments
4	Messages and transactions coming in via phone lines are serially numbered, time stamped, and logged for audit investigation and backup purposes?		
5	Employees are made aware of their responsibility to keep remote access codes secure from unauthorized access and usage?		
6	Removal of portable computers from the corporate locations must be done through normal property removal procedures?		
7	Employees are briefed on their responsibility to protect the property of the company when working away from the corporate environment?		
	VII. Company Information		
	A. Public Information		
1	Is the company publicly traded?		
2	Is the company bonded?		
3	Are all employees in the continental US? If not please list.		
	B. Private Information		
1	Are there any planned acquisitions in the next 12 months?		
2	Are there current plans to sell the company in the next 12 months?		