



**Request for Proposals
Cybersecurity, Compliance, and Managed Services**

Issued by:

Alabama Primary Health Care Association
8244 Old Federal Road
Montgomery, AL
www.alphca.com

RFP #9302026-2

Issued: October 1, 2026
Proposals Due: November 6, 2026

Proposals should be submitted via email to:

Erin Harvey, eharvey@alphca.com

Subject: RFP#9302026-2, RHTP Cybersecurity Services

Table of Contents

1. Introduction and Project Background.....	4
2. Procurement Method and General Instructions	4
3. Procurement Schedule.....	6
4. Proposal Content Requirements.....	6
4.1 Executive Summary	6
4.2 Respondent Contact.....	6
4.3 Organization and Responsibility Information.....	6
4.4 Cybersecurity Services Experience	7
4.5 Project Staffing	7
5. Required Service Approaches and Technical Scope.....	7
5.1 Approach A: Independent One-Time Cybersecurity Audit without Remediation Support.....	7
5.2 Approach B: Monthly Compliance Assessment, Ongoing Monitoring, Management and Advisory Service.....	8
5.3 Approach C: All-Inclusive Full Managed or Co-Managed Monthly Bundle Services.....	9
5.3.1 Full MSP Model.....	9
5.3.2 Co-Managed or Augmented IT Model.....	9
5.3.3 Standard Technology Stack.....	9
5.4 Approach D: One-Time Cybersecurity Audit with Remediation Labor	10
5.5 Cross-Cutting Technical Requirements	10
6. Year One Scope, Deliverables, and Acceptance.....	10
6.1 Year One Base Scope.....	10
6.2 Required Base Activities.....	10
6.3 Roles and Responsibilities	11
6.4 Deliverables and Acceptance	11
7. Implementation, Reporting, and Support.....	12
7.1 Reporting	13
7.2 Support and Service Levels	13
8. Clients, References, and Past Performance	13
9. Cost Proposal and Pricing Schedules.....	14
9.1 Device-Level Pricing	15
9.2 Recurring Service Price Schedule	15
9.3 Third-Party Subscription Reference Schedule.....	15
9.4 Situational Adjustments.....	16
10. Terms, Conditions, and Federal Requirements	16
10.1 Data, Privacy, and Security Terms.....	19
10.2 Federal Contract Provisions.....	19
11. Evaluation and Award Methodology.....	20
11.1 Minimum Qualifications and Responsiveness, Pass/Fail	20
11.2 Evaluation Criteria	20
12. Informational Environment Profile.....	20

Attachments

Attachment 1: Proposal Checklist and Required Certifications.....	22
Attachment 2: Vendor Certification, Assurances, and Eligibility Disclosure Form.....	28
Attachment 3: Approach A: One-Time Cybersecurity Assessment without Remediation Support Pricing	31
Attachment 4: Approach B: Monthly Assessment, Compliance Management and Ongoing Monitoring Pricing.....	32
Attachment 5: Approach C: All-Inclusive Managed/Co-Managed Monthly Bundle with Device-Level Pricing.....	33
Attachment 6: Approach D: One-Time Cybersecurity Audit with Remediation Labor Pricing.....	34
Attachment 7: Third-Party Pass-Through Subscription Reference Schedule.....	35
Attachment 8: Situational Adjustment and Optional Unit-Price Schedule	36
Attachment 9: Implementation Timeline and Responsibility Matrix	37
Attachment 10: Federal Contract Provisions and Certifications	42
Attachment 11: Required Cost Proposal Form.....	47

1. Introduction and Project Background

The Alabama Primary Health Care Association (APHCA) represents the operational, clinical, and financial interests of community health centers. Alabama health centers collectively serve more than 330,000 medically underserved patients annually across 217 community locations. APHCA supports quality, population health, patient and staff experience, operational performance, and cost efficiency across its integrated network.

Through this RFP, APHCA seeks scalable cybersecurity, compliance, and information-technology support services for participating rural healthcare organizations under APHCA's Pathway to Intelligent Care Rural Health Transformation Program (RHTP) initiative. APHCA seeks proposals across a continuum of service models, ranging from independent one-time assessments to fully managed or co-managed monthly programs that may include compliance management, monitoring, remediation, technical support, project and engineering services, and third-party subscriptions.

The Year 1 base scope is expected to support six participating rural healthcare organizations: four federally qualified health centers and two rural health clinics, operating across approximately 29 care locations and supporting approximately 56 providers. Final organizations, environments, assets, users, endpoints, tenants, and configurations will be validated during contracting and onboarding.

Services beyond the Year 1 base scope are optional and are not guaranteed. Any continuation, expansion, or option exercise is contingent on documented program need, available funding, satisfactory contractor performance, applicable eligibility, ADECA prior approval when required, and compliance with procurement and contracting requirements.

2. Procurement Method and General Instructions

APHCA is conducting this procurement as a competitive procurement using simplified acquisition procedures for competitive proposals under 2 CFR §200.320(a)(2). The estimated aggregate value of the proposed contract falls below APHCA's documented simplified acquisition threshold. This procurement is conducted in accordance with 2 CFR §§ 200.318 through 200.327, APHCA's written procurement policies, applicable Alabama requirements, the RHTP award, and ADECA requirements. Before award, APHCA will document the procurement method, anticipated aggregate contract value, price reasonableness, contractor responsibility, required approvals, and basis for award. APHCA seeks proposals in response to RFP #9302926-2 to procure revenue cycle software with artificial intelligence as part of the Rural Health Transformation Program supported by the Centers for Medicare and Medicaid Services (CMS) of the U.S. Department of Health and Human Services (HHS) and as part of a financial assistance award, with 100 percent funded by HHS/CMS and 0 percent funded by non-governmental sources. The contents contained in the RFP are those of the Alabama Primary Care Association and do not necessarily represent the official views of, nor an endorsement by, HHS/CMS or ADECA.

APHCA will maintain a procurement history documenting the solicitation and amendments; sources solicited; proposals received; evaluator conflict-of-interest certifications; responsiveness and responsibility reviews; evaluation criteria; individual and consensus scoring; clarifications, demonstrations, and best-and-final offers; price or cost analysis; exclusion screening; selection; negotiations; approvals; and the basis for award. Consistent with 2 CFR §200.321, APHCA has considered and, to the extent practicable, solicited small and disadvantaged business responses in connection with this procurement.

This RFP is a solicitation and does not constitute an offer or contract. APHCA may issue a conditional notice of intent to award. No contractual rights arise unless all required approvals are received, and APHCA and the selected vendor execute a written agreement.

APHCA will submit the proposed agreement, scope, pricing, and supporting documentation to ADECA for prior written approval. APHCA will not execute an agreement before the required review period concludes and it receives all approvals.

Any conditional notice of intent to award does not guarantee a purchase, minimum agreement terms, transaction volumes renewal, expansion, or future funding. Any executed agreement will be limited to the scope, term, pricing, and funding stated within the executed agreement. APHCA may make an award or no award. APHCA will not order services outside the competed scope unless a separate compliant procurement or other authorized method is documented and approved.

Specifications are minimum operational, interoperability, privacy, security, and performance requirements and are not intended to favor a vendor. Each named product, platform, or feature shall be read as “or functionally equivalent,” unless expressly identified as a mandatory compatibility requirement. Respondents must disclose actual, potential, or perceived independence impairments arising from assessing, remediating, monitoring, or validating the same environment and must describe safeguards used to preserve objectivity.

Submit all questions about this RFP and subsequent process via email to **Erin Harvey at eharvey@alphca.com by October 9, 2026**. APHCA will not accept phone calls or oral questions; do not direct inquiries to APHCA staff or member health centers outside of the process established above. APHCA will distribute addenda and written responses equitably to known recipients. APHCA will answer questions deemed relevant to the RFP by October 14.

The following section provides instructions for preparing a response that enables vendors to address the technical, financial, and legal requirements of this RFP. Vendors must read the directions carefully, follow the provided format and numbering scheme, and answer every question. For any question that does not apply, vendors should respond, “N/A.”

Respondents should certify that they maintain written conflict of interest, information security, privacy and record retention controls appropriate to the proposed services. Vendors should further certify that neither the organization, its principals, nor proposed subcontractors are suspended, debarred, excluded, or otherwise ineligible to participate in federally funded

programs and agree to maintain eligibility throughout the performance period. If selected, respondents agree to comply with all applicable federal, HHS, CMS, RHTP, ADECA, and contractual requirements incorporated into the resulting agreement.

3. Procurement Schedule

To support the anticipated selection and implementation timeline, APHCA intends to operate according to the following schedule:

Activity	Date
RFP release	October 1, 2026
Questions due	October 9, 2026
Answers/addenda issued	October 14, 2026
Proposal due	November 6, 2026, 4:30 p.m. CT
Conditional intent notice	November 13, 2026
Proposed agreement submitted to ADECA	November 13, 2026
Anticipated execution, subject to approvals	November 30, 2026

APHCA reserves the right to make modifications to the above schedule at its sole discretion. In the event of significant change(s), Vendors will be notified by email.

4. Proposal Content Requirements

4.1 Executive Summary: Provide a high-level synopsis of the vendor's response to the RFP, including:

- Proposed service approach or approaches
- Implementation strategy and schedule
- Support and escalation model
- Key deliverables and expected benefits
- Material assumptions, dependencies, and exclusions

4.2 Respondent Contact

- Name and title
- Email and telephone number

4.3 Organization and Responsibility Information

- Legal name, DBAs, registration state, headquarters, founding year, ownership history, and taxpayer identification number
- Corporate principal authorized for exclusion screening
- Nonprofit, healthcare, and multi-site experience
- Organizational chart and proposed subcontractors
- Litigation, regulatory, breach, investigation, enforcement, termination, or material claim disclosures for the prior five years

- Insurance coverage, limits, deductibles, and carrier ratings
- Written conflict-of-interest, information-security, privacy, records-retention, and business-continuity controls
- Completed and signed Attachment 10: Federal Contract Provisions and Certifications, including all required federal eligibility, exclusion-status, lobbying, and other applicable disclosures

4.4 Cybersecurity Services Experience

- Year organization began providing cybersecurity services
- Describe your nonprofit, healthcare, and/or multi-site client base experience and related scopes of service provided
- Identify contractors or subcontractors involved in service delivery
Describe any cybersecurity-specific certifications held by your organization and other advanced recognition, licensing, or certifications that support your capability under the proposed scope of work

4.5 Project Staffing

- Project executive and account lead
- Security assessment lead
- GRC/compliance lead
- SOC and incident-response lead
- Engineering and remediation lead
- Help-desk and infrastructure-management lead, if applicable
- vCIO/vCISO lead, if applicable
- Qualifications, certifications, tenure, location, availability, and assigned responsibilities

5. Required Service Approaches and Technical Scope

Respondents may propose one or more approaches. Each proposed approach must be independently understandable and priced using the required schedules. APHCA may combine approaches only through the evaluated award and approved contract.

5.1 Approach A: Independent One-Time Cybersecurity Audit without Remediation Support

Under Approach A, the contractor acts as a third-party assessor and does not provide ongoing technology, monitoring, or remediation services under the engagement. Pricing must be a one-time, all-inclusive fixed fee.

- HIPAA Security Rule risk analysis and technical evaluation
- NIST CSF 2.0 maturity and gap assessment
- CIS Controls crosswalk, when applicable
- Asset, network, identity, endpoint, cloud, and security-control review
- External and internal vulnerability assessment
- Authorized external and internal penetration testing
- Web application testing
- Wireless security assessments

- Access-review methodology
- Audit-logging control assessments
- Detailed phishing-simulation methods
- Microsoft 365, Entra ID, Defender, Intune, and cloud-security review, when applicable
- Incident-response and business-continuity readiness assessment
- Third-party risk review
- Risk register, vulnerability inventory, findings report, executive briefing, and prioritized remediation roadmap
- On-site inspector or assessment appliance deployment for approximately two to four weeks when proposed, followed by retrieval or secure decommissioning
- Assessment findings report with risk identification, stratification, and recommendations for remediation

The proposal must explain the assessment, appliance, data collection, storage location, encryption, access, chain of custody, return, sanitization, and destruction procedures. The base price must include all labor, testing, appliance, shipping, travel, reporting, and related expenses. Remediation and post-report support are excluded unless they are separately priced and authorized. Because Approach A is a point-in-time engagement, corrective actions completed after the final assessment are not considered independently verified unless remediation verification or retesting is separately included, priced, authorized, and completed.

5.2 Approach B: Monthly Compliance Assessment, Ongoing Monitoring, Management and Advisory Service

Approach B provides recurring governance, risk, compliance, assessment, and advisory services. APHCA or the participating organization remains responsible for remediation unless separately ordered.

- Vendor-managed GRC platform with direct authorized client access
- Ongoing quarterly risk assessments, control management, evidence collection, risk-register maintenance, and compliance mapping
- Compliance-readiness support for HIPAA, NIST CSF 2.0, CIS Controls, PCI DSS when applicable, and CMMC only when contractually applicable
- Policy, process, procedure, and operational-framework support
- Executive, technical, and governing-board dashboards
- Recurring vulnerability scanning at least every six months and more frequently when risk or material change warrants
- Periodic penetration testing, social-engineering testing, and remediation verification as expressly included
- Security-awareness and phishing-simulation services
- Identity and dark-web monitoring
- Microsoft 365 governance and SaaS security monitoring
- Other cloud service model monitoring including AWS, Azure, and Google Cloud services
- All required licensing, subscriptions, technical labor, reporting, and advisory services

For each recurring approach, the respondent must identify whether external vulnerability scanning is continuous or periodic; whether penetration testing is quarterly, annual, or otherwise scheduled; the entity performing each activity; that entity's independence from implementation and managed operations; and any additional charge required to maintain the proposed cadence. The contractor supports compliance readiness and evidence management but does not guarantee legal or regulatory compliance. Each participating organization retains responsibility for risk acceptance, policy decisions, safeguards, corrective actions, and compliance determinations.

5.3 Approach C: All-Inclusive Full Managed or Co-Managed Monthly Bundle Services

Approach C combines compliance management, dedicated or co-managed support, monitoring, remediation, project and engineering work, and a defined standard third-party subscription stack required for the proposed HIPAA-aligned operating model.

5.3.1 Full MSP Model

- End-to-end infrastructure management
- Security operations and monitoring
- Help desk and escalation
- vCIO and/or vCISO leadership
- Endpoint, identity, cloud, network, firewall, backup, and continuity support
- Incident-response support
- Ongoing remediation, engineering, retesting, and reporting

5.3.2 Co-Managed or Augmented IT Model

- Vendor operates alongside participating organizations' internal IT teams
- Proposal identifies retained, vendor, and shared responsibilities
- Coverage hours, escalation, privileged access, change authority, incident command, service boundaries, and required client staffing are expressly defined
- Model augments existing capacity and does not replace internal staff unless expressly selected and authorized

For a substantially equivalent scope, technology stack, service levels, and deliverables, respondents must identify whether pricing differs between the full MSP and co-managed or augmented IT models. State any difference separately and support it with the responsibilities, staffing, tools, or services that drive the adjustment. When other technology vendors remain involved, including EHR, telecommunications, copier, internet-service, cloud, or specialty-system vendors, the respondent must describe its vendor-management role, escalation responsibilities, coordination procedures, and methods for maintaining transparency regarding ownership, status, dependencies, and resolution of cross-vendor issues.

5.3.3 Standard Technology Stack

- Compliance-management suite
- Microsoft 365 services or applicable security add-ons

- Advanced email protection
- SaaS alerting engine
- Managed SOC service
- Management agents
- Security agents, including EDR/XDR
- Firewall as a service
- Any functional equivalent product must be clearly identified and mapped to the required function

5.4 Approach D: One-Time Cybersecurity Audit with Remediation Labor

- Assessment and remediation
- Penetration testing and social-engineering testing
- Microsoft 365, Entra ID, Defender, or Intune hardening
- Network segmentation and firewall implementation
- Endpoint, server, or identity remediation
- Backup, disaster-recovery, and continuity improvements
- Incident-response planning and tabletop exercises
- Policy and procedure development
- Remediation verification and retesting
- Emergency incident response and digital forensics

5.5 Cross-Cutting Technical Requirements

- Security operations center and SIEM capabilities
- 24x7x365 monitoring options and defined alert escalation
- Endpoint detection and response
- Network, cloud, email, identity, and ransomware detection
- Asset inventory and configuration management
- Infrastructure hardening and vulnerability management
- Backup, restoration, disaster recovery, and business continuity
- Incident response, digital forensics, ransomware recovery, and communications
- HIPAA, NIST CSF 2.0, CIS Controls, SOC 2, ISO 27001, PCI DSS when applicable, and CMMC when contractually applicable
- Healthcare privacy, PHI/PII handling, business associate agreements, and secure data exchange
- Security awareness, role-based training, peer learning, and technical assistance

6. Year One Scope, Deliverables, and Acceptance

6.1 Year One Base Scope

The Year 1 base scope covers six rural healthcare organizations (operated by five corporations), approximately 29 care locations, and approximately 1100 devices. Final technical quantities will be confirmed through an anonymized environment profile, contracting, and onboarding.

6.2 Required Base Activities

- Kickoff, discovery, implementation planning, and scope validation
- Current-state technology, network, cloud, identity, endpoint, security-control, and EHR-supporting environment inventory
- Organization-specific HIPAA risk analysis and NIST CSF 2.0 maturity assessment
- Internal and external vulnerability assessment and authorized penetration testing
- Microsoft 365 and cloud-security review when applicable
- Risk register, prioritized vulnerability inventory, and remediation roadmap
- Incident-response and business-continuity readiness assessment
- Incident-response plan development or improvement support
- Tabletop exercise and after-action report
- Security awareness and role-specific training
- Monitoring, threat management, alert escalation, compliance tracking, and remediation according to the selected package
- Monthly executive, technical, risk, remediation, performance, and RHTP reporting
- Remediation verification or retesting
- Final Year 1 maturity and improvement report for participating RHTP facilities
- Source documentation supporting APHCA monitoring, invoice review, deliverable acceptance, and RHTP reporting

6.3 Roles and Responsibilities

APHCA will select participating organizations; approve sequencing and priorities; coordinate participation agreements; review findings; establish program priorities; monitor performance; accept deliverables; and authorize payment. The contractor will perform only the contracted technical, assessment, monitoring, remediation, documentation, reporting, training, and support services. The contractor may not select beneficiaries, control RHTP funds, establish APHCA policy, approve its own deliverables or invoices, determine APHCA's official results, or make final programmatic decisions.

Where the contractor assesses or validates controls it implemented or manages, it must use disclosed independence safeguards, including separate personnel, independent quality review, documented methodology, evidence retention, and APHCA approval. APHCA may obtain separate independent validation.

6.4 Deliverables and Acceptance

Deliverable	Minimum Acceptance Basis
Risk register	Complete, prioritized, traceable to evidence and responsible party
Vulnerability inventory	Asset, severity, source, status, recommended action, and due date
Remediation roadmap	Risk-based sequencing, dependencies, estimated effort, and verification method
Security maturity assessment	Documented methodology, baseline, gaps, and target state

Executive dashboard	Current risk, trends, actions, exceptions, and decisions
Compliance gap analysis	Framework mapping, evidence, gap, owner, and corrective action
Incident-response plan	Roles, escalation, communications, recovery, and testing
Assessment report	Scope, methods, findings, limitations, evidence, and recommendations
Penetration-test report	Rules of engagement, methods, findings, exploitation evidence, and remediation
Monthly report	Monitoring, alerts, vulnerabilities, remediation, service levels, and exceptions
Final Year 1 report	Outcomes, maturity change, unresolved risk, sustainability, and source documentation

Given the federal and state reporting and documentation requirements of the Rural Transformation Program, APHCA may treat incomplete, inaccurate, unsupported, late, or nonconforming deliverables as a material breach if not remedied within two business days, or if such failure results in program penalties, reimbursement ineligibility, or other adverse impact on APHCA's ability to deliver program documentation timely. Upon such occurrence, Respondent will be responsible for economic injury incurred by APHCA.

7. Implementation, Reporting, and Support

Before deploying an assessment appliance, management agent, security agent, firewall, or related tool, the contractor must coordinate required firewall rules, antivirus or endpoint-security exceptions, network access, privileged credentials, site access, shipping, and approved change windows in writing with the participating organization's authorized contact. The implementation schedule must identify which party is responsible for each prerequisite and the effect of delays on milestones and pricing.

For each proposed approach, provide a phased implementation schedule that includes the following steps and identifies duration, responsible party, dependencies, client inputs, deliverables, acceptance criteria, data handling, and pricing assumptions.

- a. Contract activation and readiness review
- b. Kickoff, discovery, and scope validation
- c. Environment and access inventory
- d. Inspector-appliance preparation and shipment, when applicable
- e. Site implementation window
- f. Deployment and configuration
- g. Initial data collection and control review
- h. Scanning, testing, and validation
- i. Preliminary findings review
- j. Initial report generation

- k. Remediation planning
- l. Remediation or advisory support according to the selected approach
- m. Retesting and verification
- n. Steady-state monthly operations
- o. Final reporting and secure offboarding

Implementation assumptions must address the availability of current policies, procedures, prior risk assessments, business associate agreements, vendor contracts, network diagrams, asset inventories, and other evidence needed to evaluate the environment. Respondents must also identify dependencies on formal change-control windows, physical-access restrictions, third-party vendor coordination, and continuity of participating-organization leadership and technical contacts, together with proposed schedule contingencies for foreseeable delays.

7.1 Reporting

Respondents should provide a description of and samples of the following:

- Executive and governing-board dashboards to include total number of alerts, percentage of alerts triaged/addressed, and total up time
- Risk-scoring methodology
- Monthly technical and service-level reports to include total number of alerts, percentage of alerts triaged/addressed, and total up time
- Cybersecurity maturity and compliance reporting
- Remediation tracking
- Trend analysis to include total number of alerts, percentage of alerts triaged/addressed, and total up time
- Additional related, routinely provided performance reports
- RHTP source documentation and invoice support (TBD after contract approval and award)

7.2 Support and Service Levels

Respondents should provide a description of their proposal:

- Coverage hours and support channels
- Severity definitions
- Acknowledgment, triage, escalation, response, and resolution targets
- Critical incident communications
- Issue tracking and unresolved-issue escalation
- Maintenance windows and uptime commitments
- Service credits or other remedies offered
- Knowledge transfer, documentation, peer learning, and training

8. Clients, References, and Past Performance

Respondents should provide at least three references for comparable nonprofit and/or healthcare, or multi-site engagements. Identify entity type, contact information, service model, duration, approximate scale, and whether APHCA may contact the reference.

For each quantitative metric, define the calculation, measurement period, number and type of clients included, baseline, endpoint, material exclusions, independent-validation status, and whether the result was vendor-controlled or depended on client action.

Metric	2024	2025	2026 YTD
Recurring managed-service client retention			
Reduction in critical/high vulnerabilities % decrease from baseline year over year			
Mean Time to Detect (MTTD) Vulnerabilities – per year			
Mean Time to Remediate (MTTR) - per year			
Closure rate of findings/recommendations			
Percentage of alerts triaged/addressed - per year			
Cybersecurity maturity improvement			
Compliance-gap closure or posture improvement			
Average Incident containment time			
System reliability “uptime” percentage			
Incident-response readiness improvement			

9. Cost Proposal and Pricing Schedules

Respondents should complete the associated cost proposal and pricing schedule attachment for each of the four service approaches included in the respective response. Additionally, the respondent must state whether remediation, project, engineering, helpdesk, and operational-support labor is unlimited within the defined scope, subject to an hourly or monthly allowance, or billed separately. Disclose any included-hour limit, overage rate, excluded activity, approval requirement, or condition that may generate an additional charge in the applicable pricing schedule.

Provide firm-fixed prices or clearly defined unit prices. Pricing must include all labor, implementation, project management, applicable hardware, appliances, shipping, travel, licensing, subscriptions, third-party charges, reporting, support, remediation, engineering, testing, secure offboarding, data return, and other costs necessary to perform the proposed

service. No undisclosed charge will be payable unless authorized through a compliant written amendment and all required approvals.

9.1 Device-Level Pricing

For each of the four service approaches, Respondents should price proposed services by approach in 25-device increments through Level 28. The four service approaches include:

- Approach A: One-Time Cybersecurity Audit without Remediation Support
- Approach B: Monthly Compliance Management and Ongoing Monitoring
- Approach C: All-Inclusive Managed/Co-Managed Monthly Bundle Services
- Approach D: One-Time Cybersecurity Audit with Remediation Labor

Respondents must define “device” and specify how workstations, laptops, servers, mobile devices, network appliances, firewalls, printers, medical/IoT devices, virtual machines, and cloud workloads are treated. For comparison purposes, respondents must price each recurring service level using clearly stated baseline assumptions for the relationship among devices, users, legal entities, physical sites, Microsoft 365 tenants, and cloud environments. Respondents must separately identify adjustments when user and device counts differ, when an organization operates multiple sites or entities, or when existing client-owned subscriptions replace part of the proposed technology stack.

9.2 Recurring Service Price Schedule

Respondents must identify any minimum commitment associated with each recurring price, including whether the quoted rate requires a one-year, three-year, or other term. Proposals must separately state renewal pricing, annual escalation, early-termination charges, transition assistance, or any price difference for a shorter commitment or optional renewal period. Year 1 annual contract value must equal one-time implementation charges plus twelve times total monthly recurring charges plus all other required Year 1 charges.

9.3 Third-Party Subscription Reference Schedule

Item Category	Item	Billing Unit	Rate per Unit
Productivity/Security	Microsoft 365 service or security add-on		
Productivity/Security	Other security service add-ons for Google Cloud, AWS, or other Cloud platform		
Email Security	Advanced email protection		
SaaS monitoring	SaaS alerting engine		
SOC	RocketCyber SOC or equivalent		
Management	Management agent		
Endpoint security	Security agent/EDR/XDR		
Firewall	FWaaS firewall		
Other:			
Other:			

For Microsoft 365 and other subscriptions, identify whether the price is a new license, upgrade, add-on, management of a client-owned license, or reseller-provided subscription. Identify credits or reductions for client-owned qualifying licenses and partial-stack customers.

9.4 Situational Adjustments

Respondents should identify and provide known and anticipated circumstances that will be applied to proposed software/license items. If additional costs apply for common situational adjustments, Respondents must identify related add-on costs. Examples may include:

- Additional physical sites – Add \$XX/month per additional site
- Additional legal entities or companies – Add \$XX/month per additional company
- Multiple Microsoft 365 tenants
- User/device-count mismatch
- Servers and cloud workloads
- Partial-stack customers and client-owned subscriptions

10. Terms, Conditions, and Federal Requirements

- APHCA may reject any or all proposals, waive immaterial informalities, request clarifications, establish a competitive range, conduct demonstrations, request best-and-final offers, and negotiate consistently with fair competition.
 - Material solicitation changes will be issued by written addendum and, when appropriate, accompanied by a deadline extension.
 - Proposal preparation costs are the respondent's responsibility.
 - The selected proposal may be incorporated into the contract.
 - Respondents may not offer gratuities or engage in prohibited contacts.
 - APHCA may withhold payment, require correction, recover overpayments, or seek reimbursement for unsupported, unallowable, noncompliant, or undelivered costs as permitted by contract and law.
1. The following apply without limitation - Communication, Questions and Request for Clarification - During the Response Period, all communication (i.e.: questions, requests for clarification, etc.) must be submitted via the email address specified in Statement of Work / Deliverables Section of this RFP. APHCA assumes no responsibility for, and Vendors may not rely on oral representations made by APHCA, unless such representations are confirmed in writing.
 2. Evaluation and Selection Procedures - APHCA will screen responses to identify Vendors meeting minimum standards and those most capable of meeting the unique needs of APHCA. APHCA may request clarifications or additional information at any time during the RFP Period. Clarifications may explain or confirm information already provided and may not materially modify a proposal unless APHCA provides the same opportunity to similarly situated vendors.

3. APHCA will present responsive proposals meeting minimum qualifications and pass/fail screening requirements to the APHCA Evaluation Committee for detailed review and scoring using the published evaluation criteria. All screening team and committee members will complete conflict-of-interest disclosures before participating.
4. APHCA will evaluate proposals through a process of independent scoring, consensus scoring, demonstration scoring, reference review, responsibility determination, and ADECA approval of recommended contracting.
5. During the Evaluation Period, APHCA may, at its sole discretion, request additional information and demonstrations by some of the Vendors. APHCA reserves the right to reject all proposals, waive minor informalities that do not materially affect scope, quality, cost, competition, or vendor standing, or issue a revised solicitation.
6. RFP Amendments - APHCA reserves the right to amend, at its sole discretion, all terms of the RFP at any time during the RFP Period without prior notice. If APHCA elects to amend any terms during the Response Period, including extending the Response Period, APHCA will notify all Vendors by email as soon as practical.
7. No Commitment to Contract - APHCA reserves the right, without limit, to accept or reject any or all response(s) to the RFP, even if all the stated requirements are met.
8. Proposal Confidentiality - It is the intent of APHCA to share no proprietary marked portion of the Vendor's proposal, except as follows:
 - a. To APHCA screening team, evaluation committee, board members, or consultants as required in the performance of their duties.
 - b. To current, future, or potential APHCA members
 - c. To payers, registries, or other entities as required to assure that the proposed system solution meets the needs of APHCA and its members.
 - d. As required by federal, state, or local statute, regulation
 - e. As required by ruling of any court having appropriate jurisdiction
 - f. With the written permission of the Vendor
 - g. Where the information is generally available to the public
9. Vendors should specifically identify proprietary information within proposals. APHCA cannot guarantee confidentiality where federal law, state law, audits, monitoring activities, court order, or funding agency requirements require disclosure.
10. Release of Claims - By submitting a proposal, the vendor agrees that it will not bring any claim or cause of action against APHCA and its members, agents, employees, consultants or officers based on any information or misunderstanding concerning the information provided in the RFP. By submitting a proposal, the vendor thereby releases APHCA and its members, agents, employees, or officers from any liability arising from any such claim or cause of action. Respondents are responsible for reviewing all solicitation documents, addenda, and written responses and for seeking clarification of

any ambiguity before the question deadline. Respondents may not rely on oral statements or informal communications not incorporated into the RFP or an official addendum.

11. Negotiation - APHCA may negotiate with more than one vendor simultaneously and award the contract, or part of the contract, to any vendor in negotiations without prior notification to any other vendor negotiating with APHCA. Vendors unwilling to consider a good-faith joint negotiation should not respond to this RFP.
12. No Contract Rights until Execution - No vendor shall acquire any legal or equitable rights regarding the contract unless and until a written contract has been fully executed by the successful vendor and APHCA and its members.
13. RFP Inclusion in Contract - It is the intention of APHCA to include a successful vendor's RFP response as an attachment to the written contract with the vendor. Vendors are warned not to include any claims or terms in the RFP that they do not want in the final contract.
14. Cost of Preparing the Proposals - APHCA is not responsible for any costs incurred by a vendor to the preparation or delivery of the RFP response or in any other activities of a respondent related to this RFP.
15. Reference Check - APHCA reserves the right to contact any reference of a vendor to assist in the evaluation of the vendor's proposal, to verify information contained in the vendor's proposal and to discuss the vendor's qualifications and the qualifications of any subcontractor identified in the proposal.
16. Information from Other Sources - APHCA reserves the right to obtain and consider information from other sources concerning a vendor, such as the vendor's capability and performance under other contracts, the qualifications of any subcontractor identified in the proposal, financial stability, past or pending litigation, and any other information, regardless of whether this information is available to the public.
17. Copyright Permission - By submitting a proposal, the vendor agrees that APHCA may copy the proposal for purposes of facilitating the evaluation. By submitting a proposal, the vendor consents to such copying and warrants that such copying will not violate the rights of any third party. APHCA may reproduce proposals solely for evaluation, procurement, audit, monitoring, and contract administration purposes.
18. Non-Solicitation – During the RFP Period, vendors are prohibited from contacting or discussing the RFP with APHCA members, or other third parties except as provided for in this document or authorized by APHCA in writing. Any violation of this provision may result in the associated vendor being removed from consideration at APHCA's sole discretion.

19. Gratuities - During the RFP Period, APHCA may remove a vendor from consideration if gratuities in the form of entertainment, gifts, monies, or ownership were offered or given by the vendor, or any agent or representative of the vendor, either directly or indirectly, to any officer or employee of APHCA and its members.
20. Vendor understands that the resulting agreement will be funded in whole or in part with federal financial assistance. The selected vendor shall comply with all applicable federal, CMS/HHS, ADECA, RHTP, and contractual requirements. APHCA may withhold payment, require corrective action, terminate the agreement, or recover amounts paid to the extent unsupported charges, nonperformance, or vendor noncompliance cause project costs to be disallowed or recovered by a funding agency.
21. The selected vendor must agree to all applicable federal, state, CMS, HHS, ADECA, and RHTP contractual provisions, including those identified within Attachment D and any additional requirements incorporated into the final agreement.
22. APHCA and each participating organization retain ownership of all data, configurations, findings, results, reports, documentation, and work product generated under the resulting agreement. The selected vendor may not sell, monetize, use for unauthorized secondary purposes, or use for external model training any data belonging to APHCA or RHTP participants. Upon termination or expiration, the vendor shall return all data and documentation in a usable format and certify destruction of retained copies, except as required by law.

10.1 Data, Privacy, and Security Terms

- APHCA and each participating organization retain ownership of their data, configurations, findings, results, risk registers, reports, and documentation.
- No sale, monetization, unauthorized disclosure, external model training, or unrelated secondary use.
- Business associate agreement when required.
- Encryption at rest and in transit; multi-factor authentication; privileged-access controls; audit logging; secure hosting; subcontractor safeguards; incident and breach notification.
- Data return, portability, retention, destruction, and secure offboarding.

10.2 Federal Contract Provisions

The resulting agreement will include applicable provisions under 2 CFR § 200.327 and Appendix II to 2 CFR Part 200; 2 CFR § 200.214 suspension and debarment; 2 CFR § 200.216 covered telecommunications and video-surveillance equipment or services; 2 CFR § 200.322 domestic preferences; applicable lobbying certifications; records access and retention; and all RHTP, CMS, HHS, ADECA, and APHCA–ADECA requirements. Contracts will include appropriate remedies, termination-for-cause and termination-for-convenience terms. Respondents must follow applicable federal requirements to approved subcontractors.

11. Evaluation and Award Methodology

11.1 Minimum Qualifications and Responsiveness, Pass/Fail

- Timely submission
- Response to every required section
- Complete pricing for each proposed approach
- Contractor eligibility and conflict-of-interest certifications
- No disqualifying suspension, debarment, exclusion, or ineligibility
- Ability to meet the implementation schedule
- Required insurance and security/privacy commitments
- Acceptance of applicable federal and RHTP requirements

11.2 Evaluation Criteria

Criterion	Points
Organizational qualifications and healthcare experience	15
Technical capability and security architecture	25
HIPAA, NIST, CIS, and GRC approach	15
Implementation, staffing, and support capacity	15
Past performance and references	10
Cost and price reasonableness	20
Total	100

APHCA will evaluate price using disclosed common scenarios, so respondents are compared on the same quantities and service assumptions. Scenarios may include small, medium, and large device tiers; the Year 1 six-organization environment; an independent assessment; a co-managed monthly program; and a fully managed bundle. APHCA will evaluate total anticipated cost, not only the lowest initial or monthly price.

Evaluators will score independently before consensus. APHCA will document scores, strengths, weaknesses, deficiencies, clarifications, demonstrations, price analysis, responsibility findings, and final rationale. APHCA may not award the contract to the lowest-priced respondent.

12. Informational Environment Profile

APHCA's anticipated Y1 RHTP scope of project is provided below along with an anonymized environment profile sufficient for comparable pricing. APHCA will validate final quantities during contracting and onboarding. Respondents must state assumptions where a quantity is unavailable.

Environment element	Estimated Profile
Participating organizations	Six
Corporate headquarters	Five
Care locations	Approximately 29
Providers	Approximately 56
Endpoints	Estimated 1,200
Assessment/penetration-testing requirements	Defined in this RFP and final rules of engagement
Related EHR solutions	ECW, Epic, Athena, Greenway, Trubridge

Attachment 1: Proposal Checklist and Required Certifications

Respondents must complete and submit Attachment 1 with their proposal responses. The checklist supports the proposal organization and APHCA's responsiveness review. It does not replace any requirement stated in the RFP and is deemed part of the required minimum responsiveness. Respondents must mark each item **Included**, **Not Applicable**, or **Exception Noted** and identify the applicable proposal section or page. An incomplete checklist or missing required certification may result in rejection of the proposal as nonresponsive.

A. RFP Submission Checklist

Required Proposal Component	Included	N/A	Exception Noted	Proposal Section/Page
1. Completed and signed Attachment 1: Proposal Checklist and Required Certifications	☐	☐	☐	
2. Executive summary identifying each proposed service approach	☐	☐	☐	
3. Respondent contact information	☐	☐	☐	
4. Legal name, DBAs, registration state, headquarters, founding year, ownership history, and taxpayer identification number	☐	☐	☐	
5. Completed and signed Attachment 2: Vendor Certification, Assurances, and Eligibility Disclosure Form.				
6. Identification of corporate principal authorized for exclusion screening	☐	☐	☐	
7. Description of nonprofit, healthcare, rural healthcare, and multi-site experience	☐	☐	☐	
8. Organizational chart and identification of proposed subcontractors	☐	☐	☐	
9. Required litigation, regulatory, breach, investigation, enforcement, termination, and material-claim disclosures for the prior five years	☐	☐	☐	
10. Insurance coverage, limits, deductibles, and carrier ratings	☐	☐	☐	
11. Description of conflict-of-interest, information-security, privacy, records-retention, and business-continuity controls	☐	☐	☐	
12. Project staffing plan, including named key personnel, qualifications, certifications, tenure, location, availability, and responsibilities	☐	☐	☐	

13. Resumes or professional profiles for proposed key personnel	☐	☐	☐	
14. Completed Attachments 3-6 as applicable related to Pricing schedules for each approach	☐	☐	☐	
15. Technical response addressing all applicable service, security, privacy, interoperability, implementation, reporting, support, and acceptance requirements	☐	☐	☐	
16. Description of all proposed products, platforms, tools, appliances, licenses, subscriptions, and functionally equivalent solutions	☐	☐	☐	
17. Disclosure of assessment, implementation, monitoring, remediation, and validation independence and related safeguards	☐	☐	☐	
18. Proposed service-level commitments, severity definitions, escalation procedures, and remedies	☐	☐	☐	
19. Completed Attachment 7: Third-Party Subscription Reference Schedule, if applicable	☐	☐	☐	
20. Completed Attachment 8: Situational Adjustment and Optional Unit-Price Schedule, if applicable	☐	☐	☐	
21. Completed Attachment 9: Implementation Timeline and Responsibility Matrix	☐	☐	☐	
22. Completed Attachment 10: Federal Contract Provisions and Certifications	☐	☐	☐	
23. Completed and signed Attachment 11: Required Cost Proposal Form which includes pricing assumptions, minimum commitments, renewal pricing, escalation terms, termination charges, transition costs, and all exclusions or potential additional charges	☐	☐	☐	
24. At least three references for comparable nonprofit, healthcare, or multi-site engagements	☐	☐	☐	
25. Past-performance metrics with calculation methods, measurement periods,	☐	☐	☐	

baselines, endpoints, exclusions, and validation status				
26. Copies of required professional, business, and cybersecurity licenses or certifications, as applicable	☐	☐	☐	
27. Evidence of current SAM.gov registration or Unique Entity Identifier, if applicable	☐	☐	☐	
28. Completed W-9	☐	☐	☐	
29. Copies of proposed standard agreements, statements of work, service-level agreements, business associate agreements, data-processing agreements, and other contractual terms	☐	☐	☐	
30. Identification of all exceptions, requested modifications, assumptions, dependencies, and exclusions	☐	☐	☐	
31. Acknowledgment of all RFP amendments and addenda	☐	☐	☐	

B. Respondent Information

Legal Name: _____

Doing Business As, if applicable: _____

Business Address: _____

City, State, ZIP: _____

Taxpayer Identification Number: _____

Unique Entity Identifier, if applicable: _____

Primary Proposal Contact and Title: _____

Telephone: _____

Email: _____

Authorized Signatory and Title: _____

C. Service Approaches Proposed

Check each approach included in the proposal:

☐ **Approach A:** Independent One-Time Cybersecurity Audit without Remediation Support

☐ **Approach B:** Monthly Compliance Assessment, Ongoing Monitoring, Management, and Advisory Service

☐ **Approach C:** All-Inclusive Full Managed or Co-Managed Monthly Bundle Services

- ☐ Full MSP Model

- ☐ Co-Managed or Augmented IT Model

☐ **Approach D:** One-Time Cybersecurity Audit with Remediation Labor

☐ Other optional service expressly permitted by the RFP: _____

D. Required Certifications

By signing below, the respondent, through its authorized representative, certifies that:

1. **Authority and Accuracy.** The undersigned is authorized to submit the proposal and bind the respondent. The proposal and all attachments are true, complete, and accurate to the best of the respondent's knowledge.
2. **RFP Review and Compliance.** The respondent has reviewed the complete RFP, including all attachments and addenda, and agrees to comply with its requirements except for deviations expressly identified in the proposal.
3. **Independent Proposal.** The proposal was developed independently and without collusion, consultation, communication, or agreement with another respondent regarding pricing, proposal content, or allocation of work, except for disclosed subcontractor or teaming arrangements.
4. **No Improper Influence.** The respondent has not offered and will not offer any gratuity, gift, payment, employment opportunity, or other thing of value to improperly influence this procurement or any resulting agreement.
5. **Conflicts of Interest.** The respondent has disclosed all actual, potential, or perceived organizational, financial, personal, and professional conflicts of interest, including circumstances that could impair the independence of assessment, implementation, remediation, monitoring, or validation activities. The respondent will promptly disclose any conflict arising after submission.
6. **Suspension and Debarment.** Neither the respondent nor its principals, affiliates, or proposed subcontractors are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in covered federal transactions. The respondent will notify APHCA immediately if its status changes.
7. **Federal and Healthcare Program Eligibility.** Neither the respondent nor any person or entity proposed to perform services is excluded from participation in Medicare, Medicaid, or other federal healthcare programs or appears on the HHS Office of Inspector General List of Excluded Individuals/Entities. The respondent authorizes APHCA to conduct applicable exclusion and responsibility screenings.
8. **Responsibility.** The respondent possesses the financial capacity, technical capability, staffing, experience, licenses, insurance, security controls, and operational resources necessary to perform the proposed services.
9. **Subcontractors and Third Parties.** The proposal identifies all known subcontractors, affiliates, hosting providers, cloud-service providers, software providers, and other material third parties expected to perform or support the work. The respondent remains responsible for their performance and compliance.
10. **Pricing.** All proposed prices are firm or are based on clearly stated, objectively measurable unit-price terms. Pricing includes all costs necessary to perform the proposed scope except charges expressly identified as exclusions or optional items. The respondent understands that undisclosed charges are not payable without a compliant written amendment and all required approvals.
11. **No Guarantee of Award or Work.** The respondent understands that issuance of the RFP does not guarantee an award, minimum purchase, service volume, option exercise, renewal, or reimbursement of proposal costs.

12. **Required Approvals.** The respondent understands that any selection or notice of intent to award is conditional and that no contractual right exists unless APHCA receives all required approvals, including ADECA prior written approval when applicable, and the parties execute a written agreement.
13. **Federal Requirements.** The respondent will comply with applicable federal statutes, regulations, executive orders, award conditions, and contract provisions, including applicable requirements under 2 CFR Part 200 and the provisions incorporated through Attachment H.
14. **Records and Audit Access.** The respondent will maintain complete financial, technical, performance, security, and source documentation for the period required by the resulting agreement and applicable law and will provide authorized access for monitoring, audit, examination, and program-integrity purposes.
15. **Confidentiality, Privacy, and Security.** The respondent will protect confidential information, personally identifiable information, and protected health information; comply with applicable privacy and security requirements; execute required business associate or data-processing agreements; and report suspected or confirmed incidents within the time required by the resulting agreement.
16. **Equal Opportunity and Nondiscrimination.** The respondent will comply with applicable federal and state equal-opportunity and nondiscrimination requirements.
17. **Lobbying and Political Activity.** No federally appropriated funds have been or will be used for prohibited lobbying activities. The respondent will complete any additional lobbying disclosure required by applicable law or the resulting agreement.
18. **Trafficking in Persons.** The respondent will comply with applicable federal prohibitions concerning trafficking in persons and will require applicable subcontractors to comply.
19. **Domestic Preference and Recovered Materials.** When applicable to the contracted goods or services, the respondent will comply with domestic-preference requirements and procurement-of-recovered-materials requirements incorporated into the resulting agreement.
20. **Changes to Representations.** The respondent will promptly notify APHCA in writing if any representation, certification, disclosure, eligibility status, staffing commitment, ownership information, or material proposal assumption changes before award or during contract performance.

E. Exceptions and Disclosures

If the respondent identified any exception, qualification, conflict, adverse disclosure, or requested modification, describe it below and reference the applicable RFP provision. Attach additional pages if necessary.

☐ No exceptions or disclosures are identified.

F. Authorized Certification

I certify under penalty of applicable law that I am authorized to make these certifications on behalf of the respondent and that the information submitted is true, complete, and accurate.

Respondent Legal Corporate Name: _____

Authorized Representative: _____

Title: _____

Signature: _____

Date: _____

Email: _____ **Telephone:** _____

Attachment 2: Vendor Certification, Assurances, and Eligibility Disclosure Form

Respondents shall certify and disclose the following:

Section 1. Organization Information

Legal business name: _____

DBA name(s): _____

Principal business address: _____

UEI number: _____

Federal Tax ID Number: _____

Primary contact information: Name: _____

Telephone: _____

Email: _____

Section 2. Debarment and Suspension Certification

Vendor certifies that they:

- Are not suspended, debarred, or otherwise excluded from participation in federally funded programs.
- Will immediately notify APHCA of any change in status.
- Consents to federal and state eligibility verification.

Section 3. Conflict of Interest Disclosure

Vendor shall disclose:

- Existing business relationships with APHCA.
- Relationships with participating health centers, rural hospitals, clinics, subcontractors, or project partners.
- Actual, potential, or perceived conflicts of interest.

Section 4. Litigation and Regulatory Disclosure

Disclosure of:

- Pending litigation.
- Material lawsuits within the past five years.
- Regulatory investigations.
- Data breaches, HIPAA violations, sanctions, or enforcement actions within the past five years.

Section 5. Insurance Certification

Vendor certifies maintenance of applicable coverage including:

- General Liability
- Professional Liability / Errors & Omissions
- Cyber Liability
- Workers' Compensation

Section 6. Federal Grant Compliance Assurances

Certification that the vendor will comply with:

- 2 CFR Part 200
- Applicable federal civil rights requirements
- HIPAA and HITECH requirements
- Applicable state and federal privacy laws
- Records retention requirements
- Audit cooperation requirements

Section 7. Subcontractor Disclosure

Identify:

- Proposed subcontractors
- Scope of subcontracted services
- Percentage of work to be performed by subcontractors

Section 8. Representations and Warranties

By signing below and submitting this Proposal, the undersigned certifies, represents, warrants, and covenants on behalf of the Vendor that:

1. **Authority to Bind.** The individual executing this Proposal is a duly authorized representative of the Vendor and possesses full legal authority to submit this Proposal and bind the Vendor to all representations, commitments, obligations, pricing, schedules, deliverables, terms, and conditions contained herein and in any materials incorporated by reference.
2. **Accuracy and Completeness.** All information, certifications, statements, pricing, qualifications, references, disclosures, and supporting documentation provided in connection with this Proposal are true, accurate, complete, and not misleading as of the date of submission.
3. **No Material Omissions.** The Vendor has not knowingly omitted any information that could reasonably be expected to affect APHCA's evaluation of the Proposal, the Vendor's qualifications, eligibility, capacity to perform, financial viability, integrity, or compliance with applicable laws and requirements.
4. **Continuing Disclosure Obligation.** The Vendor acknowledges that APHCA will rely upon the information provided in evaluating proposals and making an award decision. The Vendor assumes an affirmative and continuing obligation to promptly notify APHCA in writing of any material change, error, omission, circumstance, or development that renders any portion of the Proposal inaccurate, incomplete, misleading, or no longer current. The Vendor shall provide such notification immediately upon becoming aware of the change and, in no event, no later than five (5) business days thereafter.
5. **Duty to Update.** The obligation to disclose and update information continues throughout the procurement process and, if selected, through execution of any resulting agreement and performance of contracted services.
6. **Reliance by APHCA.** The Vendor understands and agrees that APHCA may rely upon the representations and warranties contained herein in evaluating the Proposal, determining responsibility and responsiveness, making an award recommendation, and executing a contract.

7. **Consequences of Misrepresentation.** APHCA reserves the right to reject the Proposal, terminate negotiations, rescind an award recommendation, terminate a resulting agreement, or pursue any other remedies available at law or in equity if any representation, certification, warranty, or disclosure is determined to be materially false, inaccurate, incomplete, misleading, or if the Vendor fails to satisfy its continuing disclosure obligations.

Authorized Representative Name and Title

Signature

Date

Attachment 3: Approach A

One-Time Cybersecurity Assessment without Remediation Support Pricing

Single-engagement audit and advisement for participating provider through a deployed Inspector Appliance on-site for 2-4 weeks, retrieved at the closure of the assessment period. An assessment report with findings, risk scoring (high, medium, low), and recommendations included. Remediation support is not included. Note any minimum software license term. The subscription license expense should reflect the monthly cost per device for the maximum number of devices in the category.

Level	Number of Devices	Related Subscription/ License Expense	Audit Expense	Total
1	Up to 25			
2	Up to 50			
3	Up to 75			
4	Up to 100			
5	Up to 125			
6	Up to 150			
7	Up to 175			
8	Up to 200			
9	Up to 225			
10	Up to 250			
11	Up to 275			
12	Up to 300			
13	Up to 325			
14	Up to 350			
15	Up to 375			
16	Up to 400			
17	Up to 425			
18	Up to 450			
19	Up to 475			
20	Up to 500			
21	Up to 525			
22	Up to 550			
23	Up to 575			
24	Up to 600			
25	Up to 625			
26	Up to 650			
27	Up to 675			
28	Up to 700			

Attachment 4: Approach B
Monthly Assessment, Compliance Management and Ongoing Monitoring Pricing

Continuous security assessment and compliance program 24/7/365 using a compliance management approach. Ongoing audit, advisement, and related licensing, subscription fees included and labor included; participating provider maintains the responsibility for remediation. Note any minimum software license term. The subscription license expense should reflect the monthly cost per device for the maximum number of devices in category.

Level	Number of Devices	Monthly Subscription/License Expense	Annual Expense
1	Up to 25		
2	Up to 50		
3	Up to 75		
4	Up to 100		
5	Up to 125		
6	Up to 150		
7	Up to 175		
8	Up to 200		
9	Up to 225		
10	Up to 250		
11	Up to 275		
12	Up to 300		
13	Up to 325		
14	Up to 350		
15	Up to 375		
16	Up to 400		
17	Up to 425		
18	Up to 450		
19	Up to 475		
20	Up to 500		
21	Up to 525		
22	Up to 550		
23	Up to 575		
24	Up to 600		
25	Up to 625		
26	Up to 650		
27	Up to 675		
28	Up to 700		

Attachment 5: Approach C
All-Inclusive Managed/Co-Managed Monthly Bundle with Device-Level Pricing

Full-stack monthly program structured as a Managed Service Agreement (MSA) through an all-inclusive coverage of compliance auditing, dedicated or co-managed support, ongoing remediation, project and engineering work, and the standard third-party subscription stack required for HIPAA-aligned operations. Note any minimum software license term.

Level	Number of Devices	Monthly Bundled Expense
1	Up to 25	
2	Up to 50	
3	Up to 75	
4	Up to 100	
5	Up to 125	
6	Up to 150	
7	Up to 175	
8	Up to 200	
9	Up to 225	
10	Up to 250	
11	Up to 275	
12	Up to 300	
13	Up to 325	
14	Up to 350	
15	Up to 375	
16	Up to 400	
17	Up to 425	
18	Up to 450	
19	Up to 475	
20	Up to 500	
21	Up to 525	
22	Up to 550	
23	Up to 575	
24	Up to 600	
25	Up to 625	
26	Up to 650	
27	Up to 675	
28	Up to 700	

Attachment 6: Approach D
One-Time Cybersecurity Audit with Remediation Labor

Reflect related subscription/license costs required for a single-engagement cybersecurity assessment with a compressed labor effort for remediation support, while the participating provider maintains responsibility for hardware, ongoing support, third-party subscriptions, etc.

Level	Number of Devices	One-Time Audit + Remediation Total
1	Up to 25	
2	Up to 50	
3	Up to 75	
4	Up to 100	
5	Up to 125	
6	Up to 150	
7	Up to 175	
8	Up to 200	
9	Up to 225	
10	Up to 250	
11	Up to 275	
12	Up to 300	
13	Up to 325	
14	Up to 350	
15	Up to 375	
16	Up to 400	
17	Up to 425	
18	Up to 450	
19	Up to 475	
20	Up to 500	
21	Up to 525	
22	Up to 550	
23	Up to 575	
24	Up to 600	
25	Up to 625	
26	Up to 650	
27	Up to 675	
28	Up to 700	

Attachment 7: Third-Party Pass-Through Reference Schedule

The third-party subscription stack reflects the standard set of HIPAA-aligned tools commonly required in a healthcare environment. Note the proposed billing unit per user, device, company, site location, etc. with related rate. Note any minimum software license term.

Item	Billing Unit	Rate
Microsoft 365 Services		
Google Cloud or AWS Monitoring services		
Advanced Email Protection		
SAAS Alerting Engine		
RocketCyber SOC		
Management Agents		
Security Agents		
FWaaS Firewall		
Other:		
Other:		
Other:		
Other:		
Other:		

Attachment 8: Situational Adjustment and Optional Unit-Pricing Schedule

For each item, identify the price effect relative to the applicable base schedule. Add rows when additional circumstances could affect price.

Situation	Unit Basis	Included Threshold	Add/(Credit) per Unit	One-Time or Recurring	Assumptions/ Conditions
Additional physical care site	Per site		\$		
Additional corporate or headquarters site	Per site		\$		
Additional legal entity/company	Per entity		\$		
Additional Microsoft 365 tenant	Per tenant		\$		
Additional cloud environment/subscription	Per environment		\$		
Device count exceeds included tier	Per device or next tier		\$		
Client-owned qualifying subscription credit	Per license/mth		\$		
Partial technology-stack credit	Per component/mth		\$		
Other:					
Other:					
Other:					

Attachment 9: Implementation Timeline and Responsibility Matrix

Respondents should complete this attachment for each proposed service approach. The implementation plan must describe how the respondent will transition participating organizations from contract award through implementation, testing, reporting, remediation support (when applicable), ongoing operations, and secure offboarding. The implementation schedule must:

- Identify duration for each implementation phase.
- Identify responsible parties.
- Describe required client inputs and dependencies.
- Define expected deliverables.
- Define acceptance criteria.
- Identify significant assumptions.
- Identify data handling, privacy, and security considerations.
- Identify any pricing assumptions or circumstances that could affect schedule or cost.

Service Approach Covered

- ☐ Approach A: One-Time Cybersecurity Audit without Remediation
- ☐ Approach B: Monthly Compliance Management and Monitoring
- ☐ Approach C: Full MSP Managed Services
- ☐ Approach C: Co-Managed Services
- ☐ Approach D: One-Time Audit with Remediation Labor
- ☐ Other: _____

Phase 1. Contract Activation and Readiness Review

Item	Respondent Response
Estimated Duration	
Primary Responsible Party	
APHCA Responsibilities	
Participating Organization Responsibilities	
Required Inputs	
Dependencies	
Deliverables	
Acceptance Criteria	
Pricing Assumptions	

Phase 2. Kickoff, Discovery, and Scope Validation

Item	Respondent Response
Estimated Duration	
Primary Responsible Party	
Activities	
Required Documentation	

Data Collection Methods	
Deliverables	
Acceptance Criteria	
Assumptions	

Expected activities may include:

- Project kickoff
- Final scope validation
- Stakeholder identification
- Environment review
- Technical discovery
- Implementation planning
- Communications planning

Phase 3. Environment and Access Inventory

Item	Respondent Response
Estimated Duration	
Access Requirements	
Network Inventory Activities	
Cloud Review Activities	
Identity Review Activities	
Endpoint Review Activities	
Deliverables	
Acceptance Criteria	

Phase 4. Assessment Appliance Preparation and Deployment (If Applicable)

Item	Respondent Response
Estimated Duration	
Appliance Type	
Shipping Requirements	
Installation Requirements	
Data Collection Scope	
Encryption Methodology	
Data Retention Approach	
Appliance Removal Process	
Deliverables	
Acceptance Criteria	

Phase 5. Testing, Assessment, and Validation

Activity	Included	Estimated Duration	Responsible Party
HIPAA Security Risk Analysis			
NIST CSF 2.0 Assessment			
Vulnerability Assessment			
External Penetration Testing			
Internal Penetration Testing			
Cloud Security Review			
Microsoft 365 Review			
Identity Security Review			
Incident Response Readiness Assessment			
Business Continuity Assessment			

Phase 6. Preliminary Findings and Risk Review

Item	Respondent Response
Estimated Duration	
Draft Findings Review Process	
Stakeholder Participation Requirements	
Risk Prioritization Method	
Deliverables	
Acceptance Criteria	

Required Deliverables:

- Preliminary findings summary
- Draft risk register
- Vulnerability inventory
- Initial recommendations

Phase 7. Final Reporting and Remediation Planning

Deliverable	Included	Delivery Date
Executive Summary		
Risk Register		
Vulnerability Inventory		
Compliance Gap Analysis		
Maturity Assessment		
Remediation Roadmap		
Board-Level Dashboard		
Technical Reports		

Phase 8. Remediation Services (Approach C and D)

Complete only if remediation support is proposed.

Item	Respondent Response
Scope of Remediation	
Staffing Model	
Change Control Process	
After-Hours Procedures	
Validation Methodology	
Retesting Approach	
Deliverables	
Acceptance Criteria	

Phase 9. Ongoing Managed Operations (Applicable to Monthly Service Models)

Item	Respondent Response
Monitoring Coverage Hours	
Alert Escalation Process	
Help Desk Coverage	
Advisory Services	
Reporting Frequency	
Service Level Commitments	
Executive Meetings	
Technical Review Meetings	

Phase 10. Retesting and Verification

Item	Respondent Response
Retesting Methodology	
Verification Timeline	
Closure Documentation	
Deliverables	
Acceptance Criteria	

Phase 11. Secure Transition and Offboarding

Item	Respondent Response
Data Return Method	
Data Destruction Method	
Knowledge Transfer Activities	
Credential Transfer Process	
Final Documentation Provided	
Transition Support Period	
Offboarding Fees (if any)	

Responsibility Matrix

Activity	Respondent	APHCA	Participating Organization	Shared
Project Management	☐	☐	☐	☐
Discovery	☐	☐	☐	☐
Access Provisioning	☐	☐	☐	☐
Inventory Collection	☐	☐	☐	☐
Security Testing	☐	☐	☐	☐
Findings Validation	☐	☐	☐	☐
Remediation Planning	☐	☐	☐	☐
Monitoring	☐	☐	☐	☐
Reporting	☐	☐	☐	☐
Documentation Retention	☐	☐	☐	☐
Offboarding	☐	☐	☐	☐

Implementation Assumptions and Constraints

Respondents must identify:

- Required client staffing.
- Required technical contacts.
- Required access and permissions.
- Required change-control windows.
- Third-party vendor dependencies.
- EHR vendor dependencies.
- Network vendor dependencies.
- Schedule risks.
- Conditions that could delay implementation.
- Conditions that could change pricing.
- Conditions requiring APHCA written approval.

Respondent Certification

The respondent certifies that the implementation schedule represents the proposed methodology for delivering the services described in the proposal and reflects all known assumptions, dependencies, resources, responsibilities, and implementation requirements.

Signature of Authorized Representative, Title

Date

Attachment 10: Federal Contract Provisions and Certifications

This Attachment applies to the resulting Contractor and, if applicable, to covered subcontracts only to the extent required by the applicable federal award, 2 CFR 200.327 and Appendix II to 2 CFR Part 200, applicable statutes and regulations, ADECA requirements, and the executed agreement. If applicable requirements conflict, the stricter applicable term controls unless prohibited by law. APHCA may finalize or revise clause applicability after award and review by the Alabama Department of Economic and Community Affairs (ADECA). Statutory, regulatory, award, and incorporated clause text controls over any summary in this Attachment.

Administrative, Contractual, and Legal Remedies

For a contract exceeding the simplified acquisition threshold, the agreement shall provide appropriate administrative, contractual, or legal remedies for Contractor violations or breach and state the sanctions and penalties that may apply. Remedies are cumulative and do not limit rights available by law or under the agreement.

Termination for Cause and Convenience

For a contract exceeding \$10,000, APHCA may terminate for cause upon material breach, with a reasonable cure period when appropriate, and may terminate for convenience by written notice. The notice will state the effective date and extent of termination. Contractors shall stop affected work, protect property, mitigate costs, deliver completed work, and submit a final accounting. Payment is limited to accepted work and allowable, reasonable termination costs, subject to offsets and the agreement.

Suspension and Debarment

Contractor shall not participate in a covered transaction with a party that is suspended, debarred, proposed for debarment, declared ineligible, or voluntarily excluded, except as authorized by applicable federal rules. Contractor shall verify and disclose exclusion status as required and flow this requirement to cover lower-tier transactions.

Byrd Anti-Lobbying

When the applicable federal threshold is met (currently awards exceeding \$100,000), Contractor shall provide the certification required by 31 U.S.C. 1352 and applicable regulations and shall submit Standard Form LLL for each required disclosure of lobbying with non-federal funds. Contractor shall flow the certification and disclosure requirements to covered lower tiers.

Domestic Preferences

To the greatest extent practicable and when applicable, Contractor shall provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States consistent with 2 CFR 200.322 and the award and shall include the applicable requirement in subawards and contracts.

Covered Telecommunications and Video Surveillance

Contractor shall not provide or use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology within any system, when prohibited by 2 CFR 200.216 and applicable federal award terms. Contractor shall promptly disclose any actual or suspected covered equipment or service and flow applicable restrictions to covered subcontracts.

Whistleblower Protections

Contractor shall inform employees in writing of applicable whistleblower rights and remedies and shall not discharge, demote, or otherwise discriminate against an employee for protected disclosures, consistent with 2 CFR 200.217 and applicable law.

Access to Records and Record Retention

Contractor shall provide APHCA, ADECA, the federal awarding agency, the Comptroller General of the United States, and their authorized representatives timely access to records, personnel, and other information relevant to the award as required by law and award terms. Records shall be retained for the period required by 2 CFR 200.334—generally three years from submission of the final financial report, or the applicable alternative starting date—and longer when litigation, claims, audits, property, program-income, indirect-cost, or other retention rules require.

Mandatory Disclosures

Contractor shall timely disclose in writing to APHCA all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the federal award, and all other matters required by 2 CFR 200.113, the award, or applicable law. Contractor shall require covered subcontractors to make corresponding disclosures.

Conflict of Interest and No Improper Influence

Contractor shall disclose actual, potential, or apparent conflicts of interest and organizational conflicts, comply with applicable APHCA, ADECA, award, and federal conflict requirements, and shall not offer, solicit, or accept any gratuity, kickback, contingent fee, or other improper influence in connection with this procurement or contract.

Flow-Down

Contractor shall include each applicable federal clause, certification, access right, prohibition, and reporting obligation in every subcontract or lower-tier agreement for which the requirement applies, shall monitor compliance, and remains responsible for performance by its subcontractors.

The resulting agreement incorporates by reference the Notice of Funding Opportunity for the Alabama Rural health Transformation Program Collaborative EHR, IT, and Cybersecurity Initiative; the terms and conditions of Cooperative Agreement RHTCMS332060; and all applicable requirements imposed by HHS, CMS, and ADECA, as each may be amended. In the

event of conflict between the terms of the resulting agreement and an incorporated requirement, the stricter applicable requirement controls unless prohibited by law.

Respondent Certifications and Representations

Respondent must mark Yes or No, explain every exception, and supplement their response whenever facts change. A Yes response means the representation is accurate as of signature, subject to any written exception identified below.

Certification/Representation	Yes	No
Neither Respondent nor its principals are presently suspended, debarred, proposed for debarment, declared ineligible, or voluntarily excluded from covered federal transactions; any exception is disclosed below.	☐	☐
Respondent and personnel to be assigned to APHCA responsibilities are eligible to participate in federal healthcare programs and are not excluded on the HHS-OIG LEIE; any exception is disclosed below.	☐	☐
When required, Respondent has executed the Byrd Anti-Lobbying certification and attached SF-LLL for each required disclosure.	☐	☐
Respondent will not provide or use prohibited covered telecommunications or video surveillance equipment or services and has disclosed any potential issue.	☐	☐
Respondent will comply with applicable trafficking-in-persons requirements.	☐	☐
Respondent is responsible and legally eligible to contract and perform; all	☐	☐

licenses, authority, and qualifications required for performance are or will be maintained.		
Respondent has made all required federal criminal-law, fraud, bribery, gratuity, conflict, and other mandatory disclosures.	☐	☐
Respondent will flow applicable federal requirements to covered subcontractors and monitor compliance.	☐	☐
Respondent accepts a continuing duty to update these representations promptly through proposal evaluation and contract performance.	☐	☐

Exceptions/Explanations (identify items and attach additional pages if needed):

Legal entity name: _____

UEI (if applicable): _____

SAM registration/exclusion status (if applicable): ☐ Active ☐ Inactive

☐ Not registered ☐ Exclusion disclosed

Active SAM registration is not required by this Attachment unless the award terms or APHCA/ADECA specifically require it; Respondent must disclose its registration and exclusion status accurately.

Authorized representative: _____

Title: _____

Signature: _____

Date: _____

Required Attachments from Respondent before Contract Execution

☐ Standard Form LLL, Disclosure of Lobbying Activities, when applicable.

☐ Documentation supporting any exception or explanation stated in this Attachment.

☐ Any other award-specific certification or documentation requested by APHCA or the Alabama Department of Economic and Community Affairs before execution.

Signature and Certification Block

By signing below, the authorized representative certifies, after reasonable inquiry, that the statements and disclosures in this Attachment are true, complete, and accurate; that Respondent will comply with all provisions determined applicable and incorporated into the executed agreement; and that Respondent will promptly update APHCA regarding any material change. The signer understands that a false, fictitious, or fraudulent statement may result in rejection, termination, suspension, or debarment, civil or criminal remedies, and other consequences provided by law.

Legal entity name: _____

Authorized representative (print): _____

Signature: _____

Title: _____

Date: _____

Email / Phone: _____

Attachment 11: Required Cost Proposal Form
Cybersecurity, Compliance, and Managed Services | RFP #9302026-2

MANDATORY FORM

Complete this Attachment for each service approach proposed. Enter “\$0 included” for included charges and “N/A” only when an item does not apply. Do not substitute a vendor pricing sheet. You may attach supplemental details, but this completed and signed form controls if pricing documents conflict.

1. Respondent Identification

Legal name: _____

DBA, if any: _____

Pricing contact and title: _____

Email and telephone: _____

Authorized signatory and title:

Proposal price-validity period (minimum 90 days):

2. Service Approaches Priced

- ☐ Approach A: Independent one-time cybersecurity audit without remediation support
- ☐ Approach B: Monthly compliance assessment, ongoing monitoring, management, and advisory service
- ☐ Approach C1: Full MSP all-inclusive monthly bundle
- ☐ Approach C2: Co-managed or augmented IT all-inclusive monthly bundle
- ☐ Approach D: One-time cybersecurity audit with remediation labor

3. Pricing Instructions and Procurement Controls

- Prices must be firm-fixed or based on clearly defined unit prices and stated in U.S. dollars. Disclose every assumption, exclusion, dependency, minimum commitment, tier, overage, escalation, pass-through charge, third-party fee, tax, transition charge, and early-termination charge.
- All prices must include all labor, implementation, project management, appliances, hardware, shipping, travel, licensing, subscriptions, testing, reporting, support, remediation, engineering, secure offboarding, data return, overhead, and profit required for the proposed scope unless expressly listed as an optional or excluded item.
- Complete pricing separately for every approach proposed. Each approach must be independently understandable and evaluable. Do not shift the required cost to another approach or future period.

- APHCA may verify arithmetic, request clarification that does not materially alter the proposal, and correct an obvious extension error using the stated unit price. APHCA will notify the respondent of any corrections.
- APHCA will evaluate total anticipated cost, including implementation, recurring charges, subscriptions, usage, likely adjustments, transition, and other required Year 1 charges, rather than only an initial or monthly rate.
- No cost may be incurred, and no work may begin before all required approvals and execution of a written agreement. Any future expansion, renewal, or option is contingent on documented need, available funding, satisfactory performance, applicable eligibility, required ADECA approval, and a written amendment or agreement.
- Pricing and award remain subject to APHCA's documented procurement procedures, applicable 2 CFR Part 200 requirements, applicable Alabama requirements for a nongovernmental recipient or subrecipient, RHTP award conditions, ADECA requirements, price or cost analysis, contractor responsibility review, prior approvals, available funding, and execution of a written agreement. Costs must be necessary, reasonable, allocable, consistently treated, adequately documented, and not prohibited by the award or law.
- Services beyond the evaluated and awarded scope are not guaranteed. No charge omitted from this form is payable unless authorized through a compliant written amendment and all required approvals. Respondents must not split, defer, bundle, or reclassify charges to evade a procurement threshold, competition requirement, or approval.
- The resulting contract is funded with federal funds under a federal award that does not permit administrative or indirect cost recovery. Respondent pricing must not include administrative costs, indirect costs, or indirect cost rate changes in any proposed price. Costs determined unallowable, inadequately documented, or inconsistent with 2 CFR Part 200 Subpart E will not be reimbursed.

4. Approach A: Independent One-Time Audit Without Remediation

Item	Required component	Firm-fixed price
A1	Kickoff, discovery, and scope validation	\$
A2	Assessment appliance, preparation, shipping, retrieval, and sanitization	\$
A3	HIPAA Security Rule risk analysis	\$
A4	NIST CSF 2.0 maturity/gap assessment	\$
A5	Asset, network, identity, endpoint, cloud, and control review	\$
A6	Internal and external vulnerability assessment	\$
A7	Authorized internal/external penetration testing	\$
A8	Web application, wireless, phishing, and social-engineering testing	\$

A9	Microsoft 365/Entra/Defender/Intune or applicable cloud review	\$
A10	Incident response and business continuity readiness	\$
A11	Risk register, vulnerability inventory, findings, briefing, roadmap	\$
A12	Travel, shipping, and other required expense	\$
Approach A: All Inclusive Cost		\$

Number of organizations covered: _____

Number of locations/devices covered: _____

Assessment limitations and excluded remediation:

5. Approach B: Monthly Compliance, Monitoring, Management, and Advisory

Item	Component	Billing unit	Unit rate	Qty.	Year 1 total
B1	Implementation/onboarding	one time	\$		\$
B2	GRC/compliance platform	month	\$	12	\$
B3	Risk/control/evidence management	month	\$	12	\$
B4	Vulnerability scanning and management	month	\$	12	\$
B5	Penetration/social-engineering testing	event	\$		\$
B6	Security awareness/phishing simulation	month	\$	12	\$
B7	Identity/dark-web/SaaS monitoring	month	\$	12	\$
B8	Microsoft 365 and cloud governance	month	\$	12	\$
B9	vCISO/advisory/reporting	month	\$	12	\$
B10	Other required cost	specify	\$		\$
				TOTAL YEAR 1: \$	

Included labor hours per month and categories:

Overage rate and approval requirement:

Scanning/testing cadence and whether included:

Remediation responsibility and separately billable activities:

Minimum term, renewal price, and escalation cap:

6. Approach C: All-Inclusive Managed or Co-Managed Bundle

Item	Component	Billing unit	Unit rate	Qty.	Year 1 total
C1	Implementation, migration, and onboarding	one time	\$		\$
C2	Managed/co-managed operations	month	\$	12	\$
C3	SOC/SIEM and 24x7 monitoring	month	\$	12	\$
C4	Endpoint/identity/network/cloud management	month	\$	12	\$
C5	Help desk and escalation	month	\$	12	\$
C6	Compliance/GRC/vCISO services	month	\$	12	\$
C7	Remediation, engineering, retesting	month	\$	12	\$
C8	Standard third-party subscription stack	month	\$	12	\$
C9	Reporting/training/tabletop support	month	\$	12	\$
C10	Other required cost	specify	\$		\$
				TOTAL YEAR 1: \$	

- Model priced: ☐ Full MSP ☐ Co-managed/augmented IT
- Remediation/project/engineering labor: ☐ Unlimited in defined scope ☐ Allowance of ____ hours/month ☐ Separately billed at \$____/hour
- Help-desk labor: ☐ Unlimited in defined scope ☐ Allowance of ____ hours/month ☐ Separately billed at \$____/hour

Client staffing retained and cost-driving responsibility differences:

8. Approach D: One-Time Audit with Remediation Labor

Item	Required component	Firm-fixed price
D1	All Approach A assessment and reporting	\$
D2	Included remediation labor: ____ hours	\$
D3	Microsoft 365/Entra/Defender/Intune hardening	\$
D4	Network segmentation/firewall implementation	\$
D5	Endpoint/server/identity remediation	\$
D6	Backup/disaster recovery/continuity improvement	\$
D7	Incident-response planning/tabletop/policy development	\$
D8	Retesting and remediation verification	\$

D9	Travel, shipping, tools, and other required cost	\$
	APPROACH D ALL-INCLUSIVE FIXED PRICE	\$

Remediation hourly overage rate and written-approval trigger: _____

Excluded remediation, hardware, subscriptions, or third-party work:

8. Device-Level Comparative Pricing, Levels 1-28

COMPLETE FOR EACH PROPOSED APPROACH

Duplicate this schedule if prices differ by approach or managed-service model. Define “device” below. Recurring Year 1 total must equal implementation plus 12 months of recurring charges plus all other required Year 1 charges.

Level	Devices	Implementation	Monthly service	Monthly subscriptions	Year 1	Year 1 total
1	Up to 25	\$	\$	\$	\$	\$
2	Up to 50	\$	\$	\$	\$	\$
3	Up to 75	\$	\$	\$	\$	\$
4	Up to 100	\$	\$	\$	\$	\$
5	Up to 125	\$	\$	\$	\$	\$
6	Up to 150	\$	\$	\$	\$	\$
7	Up to 175	\$	\$	\$	\$	\$
8	Up to 200	\$	\$	\$	\$	\$
9	Up to 225	\$	\$	\$	\$	\$
10	Up to 250	\$	\$	\$	\$	\$
11	Up to 275	\$	\$	\$	\$	\$
12	Up to 300	\$	\$	\$	\$	\$
13	Up to 325	\$	\$	\$	\$	\$
14	Up to 350	\$	\$	\$	\$	\$
15	Up to 375	\$	\$	\$	\$	\$
16	Up to 400	\$	\$	\$	\$	\$
17	Up to 425	\$	\$	\$	\$	\$
18	Up to 450	\$	\$	\$	\$	\$
19	Up to 475	\$	\$	\$	\$	\$
20	Up to 500	\$	\$	\$	\$	\$
21	Up to 525	\$	\$	\$	\$	\$
22	Up to 550	\$	\$	\$	\$	\$
23	Up to 575	\$	\$	\$	\$	\$
24	Up to 600	\$	\$	\$	\$	\$
25	Up to 625	\$	\$	\$	\$	\$

26	Up to 650	\$	\$	\$	\$	\$
27	Up to 675	\$	\$	\$	\$	\$
28	Up to 700	\$	\$	\$	\$	\$

Approach/model covered: _____

Definition of device and treatment of servers, mobile, network, IoT, virtual, and cloud assets:

9. Common Year 1 Evaluation Scenario

COMPARABLE PRICE REQUIRED

Price the RFP's stated Year 1 base scenario for six participating rural healthcare organizations operated by five corporations, approximately 29 care locations, and the technical quantity assumptions used in your proposal. Clearly state any conflict between device estimates and final validated quantities.

Cost driver	Evaluation quantity/assumption	Rate/basis	Extended Year 1 cost
Organizations	6		\$
Corporate entities/headquarters	5		\$
Care locations	Approximately 29		\$
Devices/endpoints	Respondent assumption:		\$
Users	Respondent assumption:		\$
Microsoft 365 tenants	Respondent assumption:		\$
Cloud environments	Respondent assumption:		\$
Network devices/firewalls	Respondent assumption:		\$
External IP ranges	Respondent assumption:		\$
Other material driver			\$

Scenario cost component	Amount
Implementation and onboarding	\$
Recurring service, 12 months	\$
Third-party subscriptions, 12 months	\$
Required assessments/testing	\$
Included remediation/engineering	\$
Travel/shipping/appliances/hardware	\$
Transition/offboarding/data return	\$
Other required Year 1 charges	\$
Less credits and discounts	(\$)

10. Third-Party Subscription and Pass-Through Disclosure

Product/service	Billing unit	Unit rate	Markup/rebate	Year 1 total
Microsoft 365/security add-on		\$		\$
Other cloud security add-on		\$		\$
Advanced email protection		\$		\$
SaaS alerting engine		\$		\$
SOC/SIEM service		\$		\$
Management agent		\$		\$
EDR/XDR/security agent		\$		\$
Firewall as a service		\$		\$
Other		\$		\$

Identify new, upgrade, add-on, client-owned, or reseller status and all client-owned license credits: _____

11. Situational Adjustments, Optional Units, and Credits

Situation	Unit basis	Included threshold	Add/(credit)	Conditions
Additional care site	per site		\$	
Additional legal entity	per entity		\$	
Additional Microsoft 365 tenant	per tenant		\$	
Additional cloud environment	per environment		\$	
Device above tier	per device/next tier		\$	

User above assumption	per user		\$	
Server/cloud workload	per asset		\$	
Client-owned subscription credit	per license/month		(\$)	
Partial-stack credit	per component/month		(\$)	
After-hours/emergency labor	per hour		\$	
Incident response/digital forensics	per hour/event		\$	
Transition/offboarding	fixed/hour		\$	
Other			\$	

12. Term, Escalation, Termination, and Payment Terms

Required initial commitment:

Renewal option and renewal price:

Maximum annual escalation: ____% or index/formula:

Early termination charge and calculation:

Transition/offboarding charge and calculation:

Invoice frequency and payment terms:

Prompt-payment or nonprofit discount:

Price hold for optional expansion:

13. Price Reasonableness and Cost Disclosure

Published commercial/list/catalog pricing reference:

Comparable customer, cooperative, GSA, or other benchmark:

Difference between proposed and standard/comparable pricing:

Subcontractors, affiliates, resellers, and share of price:

Volume discounts and exact breakpoints:

Contingent, performance, savings, or revenue-based fee formula and maximum:

Taxes included/excluded and legal basis:

Any related-party transaction or organizational conflict affecting price:

PRICE ANALYSIS SUPPORT

APHCA may use this information, proposal comparisons, market research, historical pricing, published pricing, or other appropriate methods to document price reasonableness. Respondents must provide sufficient detail to permit evaluation without revealing legally protected information beyond what the solicitation or law requires.

14. Assumptions, Exceptions, and Exclusions

- 1.
- 2.
- 3.
- 4.
- 5.

15. Authorized Cost Proposal Certification

By signing, the authorized representative certifies that this cost proposal is complete, accurate, independently developed, and binding for the stated validity period; includes all required costs except expressly disclosed optional or excluded charges; contains no undisclosed gratuity, kickback, collusive arrangement, contingent procurement fee, or improper influence; does not split, defer, bundle, or reclassify charges to avoid competition, thresholds, or approvals; provides pricing supported by records sufficient for price analysis, invoice review, monitoring, audit, and allowability review; and acknowledges that no work may begin and no contractual right arises before all required approvals and execution of a written agreement.

Respondent legal name:

Authorized representative (print):

Title: _____

Signature: _____

Date: _____

Email and telephone: _____

Compliance Note: This form is drafted for a nongovernmental recipient or subrecipient using federal financial assistance. It is intended to support competition, comparable pricing, price or cost analysis, procurement-history documentation, contractor oversight, and applicable contract controls. The executed agreement, award terms, APHCA policy, ADECA conditions, and applicable law control. Final legal and grant-administration review is required before release.