

Request for Proposals for SafeConnect Technology Development

YWCA Greater Harrisburg | Competitive technology services procurement

Issued: October 15, 2026 Questions due: October 30, 2026, 4:00 p.m. Eastern Time

Proposals due: November 16, 2026, 4:00 p.m. Eastern Time

Submit to: YWCA of Greater Harrisburg electronically via PennBid at

<https://pennbid.bonfirehub.com>. Public notice, written answers and addenda will be posted on PennBid and notification via Public Notice sent to Bidders who have registered with and downloaded documents from PennBid.

This solicitation will be publicly posted on PennBid at <https://pennbid.bonfirehub.com> and distributed equally to all known interested firms. Documents are available at no cost.

1. Invitation and project overview

The YWCA Greater Harrisburg is seeking proposals from qualified technology development firms, software development companies, application developers, and digital solution providers with demonstrated experience designing, developing, implementing, and supporting secure, user-centered technology platforms for the development of SafeConnect (SCAN), a secure, single-access platform for coordinated victim services in Dauphin and Perry Counties, Pennsylvania.

SafeConnect (SCAN), a secure, user-centered technology platform will allow victims/survivors and community partners to connect with YWCA services through mobile devices and computers. The platform should be designed primarily for ease of use on smartphones while also providing full functionality through computers and other internet-enabled devices. The system should support secure communication, service access, coordinated referrals, case management activities, virtual services, and data collection.

Preference will be given to vendors with experience developing secure platforms for human services, victim services, healthcare, nonprofit, government, or similarly sensitive service environments, particularly where confidentiality, accessibility, data security, and ease of use are critical.

The YWCA anticipates a 36-month project from October 1, 2026 through September 30, 2029, with an initial pilot targeted for July 2027 (Month 10), subject to written readiness approval. Up to approximately \$600,000 may be available for technology development, implementation, licensing, hosting, support, and related services. This is a planning allocation, not a guaranteed contract value. Vendors shall identify initial, recurring, optional, and post-project costs and propose a cost-effective solution. Contract award, schedule, and scope are contingent on funding, applicable award conditions, negotiations, and required YWCA and Department of Justice approvals.

2. Procurement schedule

Event	Date
RFP issued / public notice posted	10/15/2026
Written questions due	10/30/2026 at 4:00 p.m. Eastern Time
Answers/addenda published	11/5/2026
Proposals due	11/16/2026 at 4:00 p.m. Eastern Time
Anticipated selection and notification	12/11/2026
Anticipated contract execution and notice to proceed	Late December 2026–early January 2027, subject to required approvals

All dates are subject to written amendment. Questions and proposals must be received via PennBid by 4:00 p.m. Eastern Time on the stated date. Late proposals will not be considered. Proposals may be withdrawn, altered or otherwise modified within PennBid at any time prior to the due date and time. Submissions will be confirmed by electronic receipt; offerors are responsible for timely delivery and confirming receipt. Submit questions only via the “Ask a Question” feature in PennBid. No verbal explanation changes this RFP. Material changes affecting scope, pricing, or proposal preparation will include an appropriate deadline extension. Proposals must remain valid for at least 90 days after the due date; any further extension will require the offeror’s written agreement.

3. Current environment and design principles

The YWCA operates 24/7 crisis response and ongoing services for victims of domestic violence, sexual assault, and human trafficking through its Violence Intervention & Prevention Department. This project is intended to serve that population and expand services to all crime victims in Dauphin and Perry Counties, Pennsylvania. The YWCA also integrates additional departments and services into victim services such as legal, employment, and housing services. Casebook, Efforts to Outcomes, Access Databases, and other approved systems contain client records. The vendor must identify feasible integration methods rather than assume unrestricted access to those systems. VoIP deployment is a related project component but not required from this procurement; proposals, however, must describe integration and dependencies clearly, with separate prices for any VoIP integration included in the vendor’s scope.

The platform must support survivor choice, secure communication, confidentiality, accessibility including language access, and low-bandwidth use. The YWCA does not prescribe a brand or particular architecture. A configurable commercial product, custom build, or combination may be proposed if the offeror explains ownership, portability, support, and total life-cycle cost.

4. Required scope of work

The YWCA Greater Harrisburg seeks a qualified vendor to design, develop, implement, and support SafeConnect (SCAN), a secure, user-centered technology platform that enables victims/survivors, YWCA staff, and approved community partners to connect with services, communicate securely, coordinate care, manage referrals, and track service engagement and outcomes.

The platform should be designed primarily for ease of use on mobile devices while also providing full functionality through computers and other internet-enabled devices. The YWCA is open to vendor recommendations regarding the most effective technical architecture. The solution may include mobile applications, responsive web applications, secure portals, configurable software platforms, or a combination of technologies.

A. Discovery, Requirements, and System Architecture

The selected vendor will work with YWCA leadership and project staff, IT personnel, and selected community partners to assess program needs and develop the final technical and functional design.

The vendor shall:

- Conduct discovery sessions with YWCA leadership, direct service staff, IT personnel, and selected community partners when necessary.
- Map current and proposed workflows, including service entry, intake, consent, referrals, case management, case conferencing, general victim service provision, follow-up, service closure, and data collection/recording.
- Recommend a system architecture that supports separate but connected user experiences for victims/survivors, YWCA staff, and authorized community partners which may include law enforcement, hospitals, and coordinated entry systems for shelter/housing.
- Provide written documentation describing system requirements, data flows, proposed technical architecture, implementation and testing plans, identified project risks and mitigation strategies, and measurable criteria the YWCA will use to approve completed work.
- Document all proposed system connections and integrations, including any APIs used to exchange information with other systems, as well as hosting arrangements, licensing requirements, third-party services, security dependencies, and other technical requirements.
- Identify any features or integrations that require additional software, licenses, subscriptions, or third-party agreements.

B. Victim/Survivor Access and Services

The victim/survivor-facing platform shall provide individuals with a secure, accessible, and user-friendly way to connect with services and participate in ongoing service coordination.

Required functions shall include, at minimum:

- Mobile-friendly and web-based access to YWCA victim services 24 hours a day, 7 days a week. Platform availability does not imply continuous live availability of every service. The system shall display YWCA-defined service hours, response expectations, emergency instructions, and after-hours options, with configurable backup routing.
- A safe and accessible entry route that clearly distinguishes emergency or crisis resources from routine service requests.
- Ability to request and receive assistance, appointment scheduling, reminders, advocacy, counseling, case management, referrals, and other available services.
- Secure two-way text or chat-based communication, calls, and secure face-to-face video communication to access services and maintain ongoing service continuity.
- Ability to participate in case conferencing and coordinated service planning when authorized by the victim/survivor.
- Support configurable backup coverage so that when the primary assigned or on-duty staff member is unavailable, engaged with another client, or unable to respond within an established timeframe, the request or communication can be automatically or manually routed to a designated backup staff member or coverage team.
- Language translation for platform content and text communications, and interpretation support for telephone and video interactions. Vendors shall identify automated translation features, qualified interpreter access, supported languages, confidentiality safeguards, and separate costs.
- Accessibility features that support users with disabilities, limited digital literacy, limited bandwidth, assistive technology needs, and shared-device access.

C. Community Partner Access and Referral Functions

SafeConnect shall include a partner-facing component for authorized community organizations and service providers.

The community partner platform shall allow approved partners to:

- Contact YWCA staff regarding shelter availability, emergency placement, victim response, referrals, consultation, advocacy assistance, service coordination, or other client support needs.
- Securely communicate with YWCA staff through text/chat, regular telephone calls through VoIP, and face-to-face video communication.

- Support configurable backup coverage so that when the primary assigned or on-duty staff member is unavailable, engaged with a client, or unable to respond within an established timeframe, the request or communication can be automatically or manually routed to a designated backup staff member or coverage team.
- Submit and send referral information and documentation through a secure process to the YWCA, or from the YWCA to community provider.
- Receive confirmation that a referral or request has been received and accepted for services.
- Track referral status, including whether a referral has been received, accepted, declined, is pending, requires additional information, or has been closed.
- Participate in authorized case coordination or case conferencing when appropriate and when required client consent has been obtained.
- Utilize built-in language translation tools when communicating with YWCA staff or assisting individuals with limited English proficiency.

D. Referral, Consent, and Warm Handoff Management

SafeConnect shall include an integrated referral and consent-management process that supports coordinated service delivery while protecting victim confidentiality, privacy, and choice.

The system shall support:

- Creation and secure transmission of referrals and authorized supporting information between the YWCA and approved partner organizations.
- Electronic completion and signature of informed consent and release-of-information forms, including the ability to revoke consent.
- Electronic acknowledgment and acceptance of referrals by receiving providers.
- Tracking and documentation of referral status through acceptance, first service connection, warm handoff, follow-up, and closure, clearly distinguishing referrals sent from confirmed service connections.
- An auditable record of consent and revocation, referral activity, provider acceptance, service connections, and authorized information sharing.

E. Communication, Counseling, Advocacy, and Case Conferencing

The platform shall support secure communication and virtual delivery of all applicable YWCA services, including but not limited to counseling, advocacy, case management, and authorized multi-provider case conferencing.

Capabilities shall include:

- Secure two-way text/chat messaging, regular telephone calls through VoIP, and face-to-face video communication.

VoIP deployment is outside this procurement, but SafeConnect calling functionality and necessary integration shall be addressed. Vendors shall explain connections to existing telephone services, dependencies, separately itemized costs, and whether individuals can participate using an ordinary telephone without installing an application.

- Service-related notifications and reminders.
- Language translation and interpretation support across communication methods.

Communication and conferencing functions must be designed with victim safety, confidentiality, privacy, and ease of use as primary considerations.

Audio and video service sessions shall not be recorded. Recording and automated transcription functions shall be disabled for service delivery. Vendors shall disclose any monitoring, artificial intelligence, or analytics features, including associated data processing and controls. Authorized service documentation and activity reporting shall remain available.

F. Data Collection, Reporting, and Performance Monitoring

All components of SafeConnect shall include the ability to collect, aggregate, analyze, and report information regarding system use and service activity.

At a minimum, the platform shall track:

- Users and access: User counts and types (victim/survivor, YWCA staff, and community partner), victimization type, unique identifiers for unduplicated participant reporting, and frequency and method of access.
- Services and engagement: Services requested, individual service histories, enrollment, appointments, and engagement.
- Referrals and connections: Referral activity and status from initiation and receipt through acceptance, decline, pending status, confirmed service connection, warm handoff, follow-up, and closure.
- Platform utilization: Use of communication and service functions, including text/chat, VoIP telephone calls, video, and other tools, along with community partner utilization.
- Performance and outcomes: Additional measures established by the YWCA or required by funding sources.

Authorized YWCA staff shall be able to generate configurable reports by defined time period, service type, program, referral source, partner organization, referral status, and other relevant variables.

Data dictionaries, APIs, exports, and reconciliation with authoritative client records shall meet the requirements in Section 4.H, Integrations and Data Management.

G. Security, Confidentiality, Privacy, and Accessibility

The system must incorporate privacy and security protections appropriate for services involving victims of domestic violence, sexual assault, human trafficking, and other crimes.

At a minimum, the vendor shall:

- Control access: Provide role-based access to information and functions, minimum necessary administrative permissions, multifactor authentication for staff and administrators, and timely account deactivation and permission changes.
- Protect data: Encrypt data in transit and at rest; maintain system and user audit trails; and provide secure backup, recovery, and incident and breach-response procedures.
- Protect survivor access: Provide secure, easy-to-use individualized access through a PIN, access code, biometric authentication, or similar method so device possession alone does not permit access to confidential information; support unduplicated participant reporting; and provide discreet account recovery and reset procedures.
- Support discreet use: Provide a neutral or disguised application name, icon, or user-selectable appearance; minimize identifying information in notifications, previews, recent activity, and other device displays; offer user-controlled notifications, visibility and privacy settings, and a quick-exit or concealment feature; and accommodate shared devices and email accounts.
- Document data practices: Describe consent capture, expiration, modification, and revocation; data retention and deletion; and all vendor, subcontractor, hosting-provider, and third-party access to YWCA or client data.
- Ensure accessibility: Web interfaces shall meet WCAG 2.2 Level AA; native applications shall provide equivalent accessible functionality and testing. Provide testing evidence, assistive technology and language-access support, and a remediation plan. Launch-blocking accessibility defects shall be resolved before pilot acceptance.

H. Integrations and Data Management

The vendor shall assess potential integration with existing YWCA systems and approved tools, including Casebook, ETO, VoIP systems, and other systems identified during discovery.

The vendor shall:

- Identify available integrations, APIs, and data-exchange options.
- Clearly identify integrations that require separate vendor agreements, licensing, fees, or technical development.
- Recommend how SCAN activity should be reconciled with the YWCA's authoritative client records.

- Provide documented APIs, standard exports, and an exportable data dictionary.
- Avoid placement of identifiable victim records in general-purpose project management or collaboration systems not approved for confidential client information.
- Describe any recommended data migration or initial data import separately, including scope and pricing.

I. Implementation, Testing, Training, and Support

The selected vendor shall provide implementation and ongoing support sufficient to ensure successful adoption and operation of the system, and ongoing usage after the project period.

The vendor shall:

- Establish development, testing, and production environments.
- Conduct functional, security, accessibility, integration, and user-acceptance testing.
- Correct critical security, functional, and launch-blocking accessibility defects before pilot or production launch. Propose defect severity definitions, acceptance criteria, and deadlines for remaining defects; obtain written YWCA approval of any deferred items.
- Provide administrator and staff training.
- Provide written user guides, technical documentation, workflow documentation, and system-administration materials.
- Provide knowledge transfer to YWCA IT personnel and designated program owners.
- Identify support hours, proposed uptime, critical-incident response and resolution targets, escalation procedures, maintenance windows, incident notification timelines, and backup restoration and maximum data-loss targets. Provide security testing evidence and demonstrated recovery results before launch.
- Describe software update, patching, and release-management procedures.
- Provide a process for system changes and enhancement requests.
- Provide a complete data export and transition plan at the end of the contract to prevent vendor lock-in and ensure continuity of YWCA operations past the project period.

J. Overall Platform Approach

The YWCA's priority is a seamless, secure, and accessible technology environment that allows victims/survivors, YWCA staff, and authorized community partners to interact through appropriately designed interfaces while supporting virtual service delivery, coordinated referrals and service navigation, informed consent, secure communication, case management, case conferencing, other victim services, and meaningful data collection.

Vendors are encouraged to recommend the technical approach they believe will best meet these objectives rather than assume that SafeConnect must be delivered exclusively as a traditional mobile application.

5. Phases and acceptance deliverables

Phase	Anticipated period	Minimum acceptance evidence
Procurement, discovery and design	Months 1–5 Oct 2026 – Feb 2027	Approved requirements, workflow maps, architecture, schedule, privacy and accessibility approach.
Build and configuration	Months 5–9 Feb 2027–June 2027	Demonstrated functions, documented integration design and dependencies, test scripts, administrator documentation. Required pilot integrations must pass testing before pilot acceptance.
Readiness and initial pilot launch (with ongoing configuration)	Months 9–12 June 2027 – Sept 2027	Passed functional, security, accessibility, and integration tests; staff training; policy configuration; data validation; written go/no-go approval. Initial pilot targeted for July 2027; configuration and training continue through September 2027.
Pilot improvement	Months 10–18 July 2027 – March 2028	Documented pilot feedback, defect resolution, usage and referral reports, and revised workflows.
Expansion and operations	Months 19–36 April 2028 – September 2029	Multi-platform rollout with partner pathways, increased service levels and expansion of access, quarterly improvements, export and transition plan.

Project months are measured from October 1, 2026, rather than contract execution. Phase overlap is intentional. Initial pilot launch is targeted for July 2027, subject to written readiness

approval; configuration and training may continue through September 2027. Vendors shall identify initial pilot capabilities, later releases, dependencies, and schedule risks and may propose alternate sequencing with justification. Final milestones and payment acceptance criteria will be negotiated in the contract. The YWCA will approve each deliverable in writing; demonstration alone is not acceptance.

6. Proposal contents

Section	Required response
Executive summary	Proposed solution, distinct advantages, major assumptions, total three-year cost.
Firm and team	Legal name, ownership, years in business, project lead, staffing, subcontractors, relevant references, and capacity.
Technical approach	Architecture, functions, safety design, accessibility, integrations, hosting, security controls, data ownership and export.
Work plan	Phase schedule, deliverables, YWCA dependencies, testing, training, support, risk mitigation.
Relevant experience	At least three comparable projects where available; describe work involving confidential human services data.
Price proposal/schedule	Itemized design, building, implementation, and recurring costs, assumptions, optional items, and cost after Year 3.
Exceptions	List every exception to scope or proposed terms and the effect on price or delivery.
Assurances	Disclose actual or potential conflicts, debarment status, material litigation affecting performance, and security incidents relevant to the proposed service. Disclose whether the vendor is suspended, debarred, or otherwise excluded from federal awards or federally funded transactions. The YWCA will verify exclusion status through SAM.gov before award. The selected contractor shall provide a UEI if required by applicable award conditions or YWCA procurement requirements; a UEI requirement

Section	Required response
	will not be assumed solely from contractor status.

Submit one searchable PDF proposal and a separate price schedule in PDF or spreadsheet form electronically via PennBid at <https://pennbid.bonfirehub.com> with subject “SafeConnect Technology RFP – [Firm Name].” Limit the narrative proposal to 10 pages, excluding the cover page, table of contents, pricing schedule, resumes, references, or other supporting documents. Vendors should provide concise responses focused on the requirements of this RFP and should not include general marketing materials unless directly relevant to the proposed solution. A single point of contact must be identified. The YWCA may request a live demonstration, clarification, or best and final offer.

7. Required pricing schedule

Price all costs in U.S. dollars. Identify fixed-fee milestones, recurring fees, unit quantities, rate increases, travel, third-party licensing, assumptions, and costs after year 3. Any VoIP integrations, hosting, licensing, or other third-party costs must be separately identified and itemized and may not be included as undisclosed charges within a general development cost. State included staff, partner, and participant volumes; storage; messaging and calling allowances; interpretation costs; and overage rates if applicable. Itemize costs by grant year (October–September) and actual service commencement dates, including costs beyond September 30, 2029.

If a time-and-materials contract is proposed, the vendor must provide justification and a firm ceiling price. The vendor may not exceed the approved ceiling without a written contract amendment, and any costs incurred above the ceiling without prior written approval will be at the vendor’s risk.

8. Evaluation and selection

Factor	Points
Survivor safety, confidentiality, security, and accessibility	25
Functional and technical solution, including integration and data portability	25
Implementation method, milestones, testing, training, and support	20
Relevant experience, team capacity, and references	15

Factor	Points
Price and documented life-cycle value	15
Total	100

The YWCA will first review proposals for responsiveness to RFP requirements and determine contractor responsibility. An evaluation committee of at least three members, consisting of YWCA staff and, as needed, external subject-matter experts, will score eligible proposals using the published evaluation factors and weights. Evaluators will document their individual scores, and the committee will document its consensus rationale.

The firms submitting the three highest-scoring proposals—or all qualifying firms if fewer than three—will be required to meet with the YWCA and deliver a presentation. Presentations and any requested demonstrations will be evaluated using the published criteria and will inform final rankings.

The YWCA may conduct reference checks and negotiate with the highest-ranked firm. If negotiations are unsuccessful, the YWCA may proceed to the next highest-ranked firm or reject all proposals. Selection will be based on the proposal most advantageous to the YWCA, considering price and all other published evaluation factors; lowest price alone will not determine selection.

The YWCA will maintain documentation of the procurement method, competition, evaluations, selection or rejection decisions, negotiations, and the basis for determining price reasonableness in its procurement file.

9. Anticipated contract provisions

- Written statement of work, milestones, fixed deliverables, acceptance tests, approved change-control process, invoicing tied to accepted work, and maximum contract amount.
- YWCA control of its data and project deliverables, access to usable exports, defined rights to custom code and configuration, third-party license disclosure, transition assistance, and continuity at termination.
- Confidentiality, security safeguards, incident notification and cooperation, subcontractor approval and flow-down obligations, audit access, records retention, and insurance as negotiated.
- Compliance with applicable federal award conditions and required contract provisions, including debarment and suspension checks. Applicable federal clauses and proposed contract terms will be provided before contract execution, with an opportunity to review, price, and disclose exceptions.
- No obligation to pay proposal costs and no work authorization before contract execution and notice to proceed.

10. Reservation and communication rules

The YWCA may amend, cancel, or reissue this solicitation; waive immaterial defects consistently; verify representations; and reject any or all proposals in its interest. Offerors must disclose conflicts of interest. Contractors that developed or drafted specifications, requirements, statements of work, or invitations for bids shall be excluded from competing on the resulting procurement as required by applicable federal procurement rules. All material questions and answers will be distributed equally. The YWCA will not disclose other offerors' proposals during evaluation except as required by law or award terms.