SERVING LOW INCOME TEXANS SINCE 1948

LONE STAR LEGAL AID

Justice has no boundaries

Request for Proposal:
Cyber Risk Posture Assessment

March 2025

TABLE OF CONTENTS

Lone Star Legal Aid (LSLA) seeks proposals from qualified vendors to conduct a Cyber Risk Posture Assessment, including penetration testing, preparation of a roadmap to address vulnerabilities, and help with any policy enhancements to meet industry standards. The objective is to ensure that our organization's infrastructure is secure from cyber threats. For more information on Lone Star Legal Aid, you can visit us at https://www.lonestarlegal.org.

Should you choose to submit a proposal, you will be "Respondent" below.

RFP AND PROJECT TIMELINE

All responses to this RFP must be received no later than 5:00 p.m. (US/Central) on April 28, 2025.

Respondents must be prepared to start as soon as possible upon selection due to the time constraints of the project.

Project completion, including issue management, evaluation, final adjustments, and final reporting must occur no later than April 30, 2026.

LONE STAR LEGAL AID OVERVIEW

Lone Star Legal Aid's mission is to protect and advance the civil legal rights of the millions of Texans living in poverty by providing free advocacy, legal representation, and community education that ensures equal access to justice. LSLA is the fourth largest free legal aid provider in the United States. We serve approximately 60,000 square miles, one-third of the state, including 72 counties in the eastern and Gulf Coast regions of Texas, and four counties in southwest Arkansas. Based on the most recent Census data for our service area, there are almost 2 million people at 125% of federal poverty guidelines who are eligible for our services. Many of LSLA's clients face isolation due to limited literacy, living in rural and remote locations, and language barriers.

We have 14 offices throughout this vast service area and use a hybrid IT infrastructure of both cloud-based services and on-premise systems. Nonprofit organizations like LSLA increasingly rely on digital platforms to manage sensitive client information. This reliance, however, exposes us to risks including data breaches, ransomware, and unauthorized access. Limited internal IT staffing and outdated or absent cybersecurity policies further exacerbate these vulnerabilities.

WHAT WE NEED

As Lone Star Legal Aid (LSLA) continues to embrace emerging technologies—ranging from cloud computing to mobile solutions—we recognize the need to ensure our cybersecurity posture keeps pace with these advancements. Our organization handles sensitive legal data and serves communities that depend on our ability to provide uninterrupted, secure legal services. We are seeking proposals from qualified vendors to conduct a comprehensive Cyber Risk Posture Assessment and conduct penetration testing. In addition, the selected vendor will prepare a roadmap to address any vulnerabilities and help with any LSLA policy creation or enhancement to ensure that industry standards are met.

Key Objectives include:

1. **Cyber Risk Assessment**

- Conduct a detailed review of existing cybersecurity policies, procedures, and technology setups against standards such as NIST Cybersecurity Framework's 23 Categories.
- Include external penetration testing to uncover exploitable vulnerabilities.

2. **Strategic Roadmap & Policy Enhancement**

- Develop a phased implementation roadmap to remediate gaps and enhance security.
- Update or enhance our existing technology policies covering general technology use, cybersecurity, AI, software development, BYOD, disaster recovery, data retention, and data breach response. The policies should be appropriate for a nonprofit law firm of our size and budget and meet current industry standards.

3. **Operational and Service Delivery Improvements**

- Strengthen defenses to reduce potential service disruptions.
- Enhance client trust through improved data security and compliance with legal standards.
- Streamline internal processes and establish a culture of cybersecurity awareness.

EXPECTATIONS

LSLA will contract with a qualified vendor to perform the work as described below.

TECHNICAL SCOPE

We expect the work to be in substantially three phases with the deliverables identified below. Please estimate the percentage of total effort for each phase in your response, discuss how you would approach implementation in each phase, and feel free to recommend any additional or alternate approach.

The selected consultant will be responsible for delivering the following:

Scope of Work

A. Cyber Risk Posture Assessment

- **Documentation Review:** Evaluate current security policies, IT organizational charts, tactical plans, and previous assessments.
- **Interviews & Workshops:** Engage with key staff to understand operational processes and identify vulnerabilities.
- **Gap Analysis:** Compare existing practices against NIST Cybersecurity Framework's 23 Categories and other relevant industry standards.
- **Penetration Testing:** Conduct controlled penetration tests to identify technical vulnerabilities.
- **Assessment Report:** Prepare an initial assessment report

B. Policy Development & Roadmap Creation

- **Policy Enhancement:** Draft new or updated policies in areas including:
  - General Technology Use
  - Cybersecurity
  - Artificial Intelligence (AI)
  - Software Development

- Bring-Your-Own-Device (BYOD)
- Disaster Recovery
- Data Retention
- Data Breach Response
- Other industry or funder recommended policies

- **Roadmap Development:** Create a detailed, phased roadmap outlining priorities and timelines for remediation efforts based on findings and recommendations.
- **Training & Awareness:** Develop and deliver staff training sessions to support the adoption of new policies and protocols.

C. Reporting & Ongoing Support

- **Interim Reporting:** Provide periodic status reports during key project phases.
- **Final Report:** Submit a comprehensive final report detailing assessment findings, recommendations, the roadmap, and new or updated policy documentation.
- **Post-Implementation Review:** Offer recommendations for continuous improvement and periodic monitoring.

The vendor shall provide, at a minimum, the following deliverables:

1. **Cyber Risk Posture Assessment Report**
   - Executive Summary
   - Detailed Findings and Gap Analysis
   - Penetration Testing Results
   - Prioritized Recommendations

2. **Strategic Roadmap Document**
   - Phased implementation plan with timelines and resource requirements

3. **Revised Policy Documents**
   - Updated policies for general technology use, cybersecurity, AI, software development, BYOD, disaster recovery, data retention, and data breach response

4. **Training & Awareness Materials**
- Documentation and materials to support staff training on new protocols

5. **Final Project Report**
- Comprehensive summary of activities, deliverables, and outcomes, including post-implementation recommendations

The anticipated project duration is **10 months**. The following is a high-level timeline:

- **Months 1–2: Preparation & Planning**
  - Conduct a kick-off meeting with the selected consultant.
  - Define scope, key stakeholders, and communication plans.
  - Initiate preliminary cybersecurity assessments.

- **Months 3–4: Assessment & Initial Reporting**
  - Execute detailed cybersecurity assessments and staff interviews.
  - Draft and review an initial gap analysis report.

- **Months 5–7: Policy Development & Roadmap Creation**
  - Develop updated security policies based on assessment findings.
  - Create a phased implementation roadmap.
  - Hold workshops and training sessions with staff.

- **Months 8–9: Implementation & Review**
  - Begin implementing key components of the roadmap.
  - Monitor and adjust strategies based on feedback.

- **Months 10: Final Evaluation & Reporting**
  - Collect evaluation data and finalize the comprehensive project report.
  - Submit final financial and performance reporting to relevant stakeholders.

Communications with LSLA

Communication with LSLA on a regular basis will be important to the project's success.

Generally, LSLA expects to meet with Respondent at least weekly.

For any other communications outside regularly scheduled meetings, LSLA and Respondent commit to responding to email messages from the other by the next business day, unless circumstances prevent.

Submission Requirements

All responses must be twenty-five (25) pages or fewer (not including references and samples of comparable work), concise and well organized, and demonstrate how your proposed services, approach and methodology, experience, and terms meet or exceed LSLA's requirements. All proposals must also contain the following:

Respondent Information

1. Respondent's full name, address, telephone number, email, and website.
2. Your submission point-person. Please include title, phone number, and email address.
3. Company overview, including a brief history, mission, number of employees, and number of years in operation.
4. Client mix: tell us what percentage of nonprofit, government, and commercial clients you serve.
5. Two (2) or more recent references concerning your experience with the type of work described in this RFP. Indicate the reference's name, a brief description of the services provided, and the name, title, telephone number and email address of an individual who is knowledgeable about your work and who may be contacted by our evaluators.

Subcontractors

If subcontractor(s) are proposed to complete this project, a description of the services provided by the subcontractor(s), their location, and the Respondent's contract management process and selection criteria for subcontractors. State the percentage of work performed by subcontractor(s).

Pricing and Pricing Methodology

Please submit a single firm fixed price (FFP) bid for the work outlined above. Payment will be made upon milestone completion, and not on an hourly or time-and-materials basis.

Please estimate a percentage of overall time for each of the phases or proposed milestones in the technical scope. The total should sum to 100%. Please also include an estimate of how long in weeks you anticipate it will take to complete the milestones in the technical scope. Please explain any factors that may affect your estimate.

LSLA is a 501(c)(3) tax exempt organization.

Pricing must include all overhead costs needed to complete the work in the proposal.

Experience and References

- Describe your experience working with any non-profit organization for whom you provided a similar service.
- Specify the approximate percentage of business you received in the past year for creating custom software for customers.
- Describe your knowledge and experience with conducting risk assessments and policy enhancements related to cyber security, with a focus on experience relevant to the technical requirements, including technical scope and communications.
- Detail your quality assurance plan or process for assessment, penetration testing, policy review, and roadmap development.
- List your personnel who will manage the services provided. This list must identify a point of contact who will manage the project as a point of contact to manage business questions. Small organizations and individuals can name the same person in both roles.
- Describe your proposed project and team organization. Identify key employees and/or supervisors.
- List the certifications and credentials and experience of staff members, contractors, and subcontractors who would perform the work.
- Provide a statement on whether the Respondent or any employee of the Respondent is related by blood or marriage to an LSLA employee or resides with an LSLA employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities within the Respondent's organization of such Respondent employees.
- Describe your testing protocols, including how improvements are incorporated and retested.
- Describe your ability to meet scope requirements Section A – Technical Scope and B – Communication.
- Provide samples or descriptions (links would be great if you can provide them) of your work on other similar projects.
- Describe any methodologies tools and frameworks to be used (e.g., NIST, industry best practices).

- Describe a project schedule aligned with the provided timeline.
- Describe specific milestones for documentation review, interviews, gap analysis, policy drafting, and roadmap approval (refer to the Milestone requirements above).

Other Information

Respondents are encouraged to provide other information or material, within the 25-page limit, that it believes is relevant to LSLA's evaluation or that provides additional features or value to LSLA. Some examples of additional value may be experience with and ability to provide documentation for LSC grant reporting requirements and/or abilities or accomplishments in user experience assessment, testing, and design.

Respondents must submit responses and documents in their technical proposal in the order above. Proposals must reference each paragraph/subparagraph number along with Respondent's response as outlined above.

Preferred Method of Contact

Currently we prefer to communicate via email. As the proposal process progresses, we will make ourselves available for phone calls and possible in-person meetings. Please submit questions relating to this RFP by email to Daniel Lopez at dlopez@lonestarlegal.org. All questions and answers will be shared with all participating Respondents via LSLA's web site.

Please include "**RFP for CRPA TIP25**" in the subject line of your email when sending questions and final proposals.

Availability During RFP Response Period

The individual(s) involved in this project can typically be reached by email between 8:00 a.m. and 5:00 p.m. Central Standard Time. Please allow 24 to 48 hours for response time.

- March 28, 2025: RFP opens.
- Through April 28, 2025: Available for questions. All questions must be submitted in writing. Questions and answers will be posted to a public page along with this RFP.
- April 28, 2025, 5:00 PM US/Central: Deadline for Respondents to submit responses.

Cost of Responses Not Included in Budget

Neither Lone Star Legal Aid nor LSC will pay any contractor costs associated with preparing responses or proposals submitted in response to this RFP.

Evaluation of Proposals

The evaluation team will first evaluate the technical proposals and score them as described below. These scores will be used to create a short list of firms for further consideration; Respondents not on the short list will not be eligible for further consideration.

After the final technical proposal scores have been calculated, the price proposals will be evaluated and scored, with a total score for each Respondents to be calculated. LSLA will then select one finalist. Should LSLA and that finalist not be able to negotiate an agreement, LSLA reserves the right to select and negotiate a contract with a new finalist. Candidates not selected will be notified by email after a contract is finalized.

The total score available will be 100 points. The proposals will be evaluated using the criteria below.

- **Knowledge and experience**: Proposals will be evaluated on the certifications described in the SUBMISSION REQUIREMENTS section above and Respondent's collective knowledge and experience with technologies relevant to the project.
- **Quality of work plan submitted**: Proposals will be evaluated on the quality of the work plan submitted.
- **Quality of samples of prior work**: Proposal will be evaluated based on the quality of samples provided.
- **Proposed fees**: Proposals will be evaluated on reasonableness of proposed fees.
- **Estimate of time required**: Proposals will be evaluated on how long it is estimated to take to accomplish the project goals.

LSLA Rights

LSLA reserves the right to:

- Accept or reject any or all responses, or any part thereof.
- Waive any informalities or technicalities contained in any response received.
- Conduct discussions with respondents and accept revisions of proposals after the closing date.
- Make an award based upon various selection criteria.
- Request clarification from any respondents on any or all aspects of its proposals.
- Cancel or re-issue this RFP at any time.
- Retain all proposals submitted in response to this RFP.
- Invite some, all, or none of the respondents for interviews, demonstrations, presentations, and further discussion.

Confidentiality

During the selection and project execution phases, LSLA may give you access to LSLA's confidential or proprietary information. You agree not to use this information for your or any third-party's benefit and will not disclose this information to any person who does not have a need to know.

LSLA will not under any circumstances disclose any information submitted by Respondent to any other Respondents, except the questions and answers described above. LSLA will not disclose any information submitted by Respondent to LSLA to any other parties until after the contract is finalized.

FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) and associated federal regulations may require LSLA to disclose certain documents to the public, including portions of your proposal. Generally, LSLA will not release any documents that would cause competitive harm to a Respondent or potential Respondent.

You are encouraged to label any confidential information contained in your proposal to facilitate LSLA's ability to withhold it from disclosure.