



LEGAL AID SOCIETY
OF MIDDLE TENNESSEE AND THE CUMBERLANDS

Clarksville · Columbia · Cookeville · Gallatin · Murfreesboro · Nashville · Oak Ridge · Tullahoma

Request for Proposal (RFP): Technology Assessment & Cybersecurity Audit

Responses Due: November 14, 2025

Legal Aid Society of Middle Tennessee & The Cumberland
1321 Murfreesboro Pike
Suite 400
Nashville, TN 37217

Purpose

The Legal Aid Society of Middle Tennessee & The Cumberland (LASMTC) is seeking professional consulting services to conduct a technology assessment and cybersecurity audit. The purpose of this endeavor is to identify vulnerabilities and inefficiencies in LASMTC technology and to provide recommendations for systems improvements, security enhancements, and policies that will better equip LASMTC to use its technology securely and efficiently in its delivery of services to clients.

Introduction

LASMTC is a 501(c)(3) non-profit law firm that provides free civil legal assistance to domestic violence victims, children, senior citizens, veterans, and low-income Tennesseans. Established in 1968, LASMTC has helped thousands of Tennesseans every year with the legal issues that threaten their ability to obtain the basic necessities of life, such as food, shelter, health care, and education. LASMTC occupies 8 offices across the state of Tennessee with nearly 130 employees. Headquartered in Nashville, TN, LASMTC also has offices in Clarksville, Columbia, Cookeville, Gallatin, Murfreesboro, Oak Ridge, & Tullahoma, TN. LASMTC also allows remote workers.

LASMTC's IT infrastructure is now almost completely cloud. LASMTC still has a local server environment, but it is only housing historical information. All software used is SaaS. LASMTC leverages Microsoft 365 and Azure for numerous services. LASMTC utilizes a case management system (CMS) that is hosted in the cloud. LASMTC's phone system is a cloud-based VoIP system. Finally, LASMTC's accounting software is also cloud-hosted. The only physical devices in LASMTC offices are networking equipment - such as routers, firewalls, switches, and access points; copiers and printers; and staff laptops and peripherals.

Background

The onset of the Covid pandemic brought new technological challenges to LASMTC in its efforts to provide services to clients. The need to do remote work complicated the processes of accessing data and systems and communicating with staff or clients in a remote environment. At the start of the pandemic, LASMTC had desktop computers for each staff member; individual PBX phone systems in each office; and centralized, in-house servers performing domain control functions, file server access, and backup operations. These systems provided limited, if any, remote access to staff.



To address these concerns, LASMTC implemented various technology changes, including deployment of a cloud-based VoIP phone system across all offices, replacement of desktop computers with laptops for all full-time staff and some volunteers, and migration from in-house servers to a cloud-based environment utilizing Microsoft Azure and Microsoft 365. These changes improved LASMTC's ability to serve clients thanks to increased accessibility and mobility.

These new technologies brought about new concerns around security and use, such as how to securely access systems and data, how to protect these systems and data from threats or loss, and how to maximize efficiency of cloud-based applications and infrastructure. Additionally, the rise of AI tools in the legal and nonprofit sectors introduces further opportunities and challenges. AI solutions may enhance productivity by assisting with document review, client intake, and internal data analysis; however, they also require careful governance to address data security, confidentiality, ethical considerations, and staff training.

LASMTC seeks consulting services to provide insight into addressing these issues through an evaluation of LASMTC's technology and security, and AI posture, resulting in recommendations for improved efficiencies and risk reduction. Further, such a consultant will aid in the improvement of technology and AI usage policies that will guide LASMTC's use of systems and data around industry best practices.

Project Overview

LASMTC's has received funding from a donor to fund an information technology assessment, security audit, and related activities. These related activities include working with LASMTC to develop a roadmap to address the findings of the assessment and audit; to assist LASMTC in developing or bolstering existing policies on IT usage, governance, and disaster response using best practices; and to develop a plan to implement needed changes, configurations, or policies that will increase LASMTC's security posture and efficiency of IT usage.

Deliverables

The selected consultant shall provide the following deliverables for this project:

- 1) A project plan that sets scope of work, timelines, and dependencies
- 2) Weekly status reports to cover progress and action items needed to progress project
- 3) Technology assessment final report, to include but not limited to:
 - a. Description of LASMTC IT environment
 - b. Summary of findings from staff interviews or surveys relevant to IT staffing, usage, and satisfaction
 - c. Performing relevant activities to conduct a technology assessment.
 - d. Analysis of technology policies, procedures, and processes with recommended improvements
 - e. Technical concerns and plans for remediation.
 - f. Horizon scan to identify emerging technologies that could benefit/compliment/replace our existing technology stack.
 - g. Estimated costs for proposed remediation solutions.



- 4) Security audit final report, to include but not limited to:
 - a. Summary report on findings delivered to key personnel at LASMTC including the Deputy Director of Operations and Technology, Executive Director, and others as identified.
 - b. Detailed report on vulnerabilities in LASMTC's IT resources
 - c. Performing relevant activities to conduct an IT security audit
 - d. Policy, configuration, and software/hardware recommendations to address vulnerabilities
 - e. Estimated costs for proposed remediation solutions.

Technology Assessment and Security Audit Scope

The selected consultant will be responsible for conducting, at minimum, the following list of items related to a technology assessment and security audit:

- Recognized assessment standard to identify cybersecurity risks and prioritize remediations
- Internal vulnerability scans to identify weaknesses in LASMTC's technology configurations
- External penetration tests to find vulnerabilities in LASMTC's public facing equipment
- Social engineering penetration tests to identify vulnerabilities associated with staff
- Data privacy assessment to determine risks and liabilities of data usage
- PII scan to determine protection needs of personally identifiable information
- Dark web scan to determine risks associated with data on the dark web
- 365 secure score assessment and improvement plan
- Disaster recovery plan assessment and policy improvement recommendations
- Backup and recovery assessment
- IT governance assessment
- Identity management and access controls assessment
- Telecom evaluation
- Network documentation assessment

Implementation (Roadmap)

The selected consultant will collaborate with relevant LASMTC staff to develop an implementation plan to address the findings and recommendations of the technology assessment and security audit.

LASMTC's plan will focus on, but is not limited to, implementing changes to:

- Revising relevant policies to address findings of the report.
- Identification of short, medium, and long-term measures to address IT security risks identified by the Security Audit and Assessment report.
- Outlining a timetable for achieving milestones towards technology improvements
- Describing how each remedial measure benefits LASMTC and enhances its IT technological and security maturity.
- Prioritizing and identifying security measures in response to the findings and recommendations of the report.



- Developing new practices for staff training or policies to carry out the implementation plan to respond to the recommended changes based on the report.

Project Timeline

The project timeline is as described below. All dates have an 11:59pm CST deadline. LASMTC reserves the right to modify the schedule at its discretion:

Dates	Objectives/Milestones
RFP Dissemination - October 10, 2025 Bidder Questions Due – October 31, 2025	Contract with a consultant to perform a technology assessment and security audit: <ul style="list-style-type: none">• Create and disseminate RFP for technology assessment and security audit.• Review Responses and select qualified consultant.• Document scope of work for assessment and audit with consultant
Final submissions due – November 14, 2025 Consultant selection - November 28, 2025	
Document scope of work – December 12, 2025	
Information gathering – January 12-23, 2026	Conduct a technology assessment and security audit: <ul style="list-style-type: none">• Furnish the consultant with all necessary information required to perform the assessment and audit.• Conduct assessment and audit.• Report findings to leadership team
Assessment work – January 26 – April 30, 2026	
Assessment reports due May 8, 2026	
May 11, 2026 – August 14, 2026	Update policies and create IT roadmap to address assessment findings: <ul style="list-style-type: none">• Update existing, or create new, policies to address findings in assessment and audit report• Create an IT roadmap for investing in technology to address findings in assessment and audit report

Proposal Submission Guidelines

Please submit your proposal in PDF format as an email attachment to rfp@las.org. The proposal should include the following:

- Letterhead with company name, address and contact information.



Clarksville · Columbia · Cookeville · Gallatin · Murfreesboro · Nashville · Oak Ridge · Tullahoma

- Name, title, address and contact information, along with preferred form of contact, of the person to contact who is authorized to represent the company, agency or contractor and to whom correspondence should be directed.
- Federal taxpayer ID for the company, agency, or contractor.
- General information including number of years in business, length of time providing the proposed services, total number of clients, number of personnel and location of personnel that would work on this project.
- A brief statement of your understanding of the services to be performed.
- Describe your approach and methodology for providing these services.
- Describe how your organization is positioned to provide services listed above and a history of the experience providing similar services. Explain any history you have working with legal services organizations, including knowledge of resources available to nonprofits.
- Acceptance of LASMTC's proposed project timeline.
- Total proposed project cost itemized as appropriate.
- Provide a complete organizational chart including names, position titles, and team structure for your entire organization. In addition, identify the names of principal staff and key personnel who will provide the services. Please submit resumes or qualifications for each key staff person, summarizing their experience and expertise. Describe each person's role and responsibility with the project.
- Signature of an officer or other person who is legally authorized to bind the applicant to the proposal cost and schedule.
- Provide the name, title, address and contact information of three references for clients who you have provided the same or similar services. Provide information on the actual services provided and length of time services were provided to client. Nonprofit references, specifically related to organizations providing legal services, are preferred.
- If possible, please provide a sample report for a project of similar size and scope.

Proposal Questions

Any questions regarding the RFP must be in writing and directed to RFP@las.org in accordance with the timeline in the "Project Timeline" section. All responses to inquiries will be available upon request by proposing vendors.

Proposal Submission Deadline & Instructions

Please submit all proposals electronically to RFP@las.org with the subject line: "RFP-Technology Assessment Proposal." Please see the "Project Timeline" section of this document for information related to submission deadlines.

Evaluation Process

LASMTC staff will review proposals, conduct interviews or ask questions of the consultants, and then make a final decision. The selected consultant will be notified and is expected to enter a contract with



LASMTTC within 30 days of acceptance. Consultants whose responses are not selected will be notified via email.

Evaluation Criteria

Proposals will be evaluated based on the following weighted criteria:

Evaluation Criteria	Weight (%)
Technical Expertise & Qualifications – Demonstrated experience in IT assessments, cybersecurity, cloud environments, and AI governance, including work with nonprofits or similar organizations.	25%
Assessment Methodology & Deliverables – Quality and clarity of the proposed approach to evaluating technology, security, and AI posture; strength of analysis framework; usefulness of deliverables and recommendations.	20%
Cost & Value – Overall value of the proposal in relation to price; demonstrated cost-effectiveness.	20%
Security & AI Considerations – Ability to address data security, compliance, risk reduction, and responsible adoption of AI in nonprofit/legal aid settings.	15%
Service Flexibility & Scalability – Capacity to adapt recommendations to LASMTTC's size, resources, and evolving needs, with scalable solutions for future growth.	10%
Organizational Fit & Values Alignment – Understanding of LASMTTC's mission, culture, and priorities; ability to partner effectively with staff and leadership.	10%
TOTAL	100%

Budget & Funding Parameters

This project is supported by a grant that provides up to \$35,000 for a comprehensive technology assessment.

Proposals should reflect the full scope of services the vendor believes are feasible and appropriate within this budget.

The organization may consider proposals that include optional add-ons or phased approaches beyond this amount; however, any costs exceeding \$35,000 would require separate funding approval and are not guaranteed.

While the full \$35,000 is available, vendors are encouraged to submit cost-effective proposals that deliver the greatest value and actionable outcomes within that limit.



General Terms and Conditions

- All costs associated with responding to this RFP are the sole responsibility of the responding Provider.
- Proposals submitted in response to this RFP become the property of LAS. LAS reserves the right to use any and all ideas included in any proposal without incurring any obligations to the responding consultant or committing to procurement of the proposed services.
- LAS reserves the right to reject any or all proposals.
- A short-term agreement may be executed initially, with potential for extension.
- Specific terms and conditions of contract to be determined after a conditional offer is made by LAS and accepted by the selected consultant.
- The selection of a vendor pursuant to this RFP does not constitute an endorsement of the vendor's services. The vendor agrees to make no reference to LAS in any literature, promotional material, brochures, sales presentations, or the like without the express written consent of LAS.

Procurement, Compliance, & Data-Security Requirements

LAS will conduct this solicitation under its **Accounting Manual purchasing rules** (competition threshold \$25 000; minimum three bids; conflict-of-interest notice) and **all Legal Services Corporation (LSC) regulations**. Offerors should be aware that, if amendments cause cumulative LSC-funded spend to exceed \$25,000, LAS must secure **prior written approval from LSC**. Vendors may be asked to furnish supporting cost documentation to facilitate that request.

Competitive solicitation. Consistent with LAS Accounting Manual procedures, this RFP will be distributed to and/or publicly posted to ensure evaluation of no fewer than three qualified vendors. Any request for non-competitive selection must meet the exception criteria and obtain written approval from the Executive Director.

Conflict-of-interest (COI) notice. As bids are received during the vendor selection process, LAS will email the vendor's name and project summary to applicable employees, volunteers, and Board members. Recipients are required to disclose potential conflicts to the vendor selection committee for verification. Disclosures and determinations will be stored with the procurement file.

Data Security Requirements. Vendors should expect to adhere to LAS technology standards as documented in the LAS Technology Policy.