Request for Proposals

Security Assessment and Penetration Testing

Issued by: Kentucky Legal Aid (KLA)

RFP issue date: November 17, 2026

Questions due: December 7, 2026
Submit questions to: Rehman Khalid, vCIO, Kentucky Legal Aid, rkhalid@klaid.org

Proposals due: December 14, 2026 at 5:00 pm CST
Submit proposals to: Sarah Hayes, Kentucky Legal Aid, Grants | Pro Bono Director, shayes@klaid.org

1. About KLA and the Project

Kentucky Legal Aid is a regional nonprofit public-interest law firm that provides civil legal services to low-income and other vulnerable people in 35 counties in southcentral and western Kentucky. KLA is the area's Legal Services Corporation-funded legal services provider, and more than 80% of its service area is rural. KLA is headquartered in Bowling Green, with regional offices in Paducah, Owensboro, and Madisonville and satellite offices in Glasgow, Scottsville, and Hopkinsville.

KLA completed a security assessment in July 2023. Since that time, KLA has made significant changes to its technology environment, including replacement of its firewall infrastructure, adoption of cloud-based management for all staff devices, a transition to passwordless authentication and automated device provisioning, and the ongoing retirement of its on-premises server in favor of Microsoft 365 and SharePoint. As a result, the 2023 assessment no longer reflects KLA's current security posture.

KLA staff handle confidential client information every day. KLA now seeks a security assessment, conducted from an attacker's perspective, to identify exploitable weaknesses before they can be used against the organization. This engagement will be coordinated with KLA's separately procured Technology Assessment and Technology Improvement Plan. The security assessment will identify security vulnerabilities and prioritized remediation needs, while the separate technology assessment will focus on optimizing KLA's use, integration, staff adoption, training, governance, user support, reporting, and documentation within its existing core technology platforms. Findings from both engagements will inform KLA's Technology Improvement Plan.

2. Purpose and Scope

KLA seeks a qualified security firm to conduct a black-box security assessment. The selected firm will begin with only KLA's organization name and public website (www.klaid.org). KLA will not provide network diagrams, IP address ranges, staff directories, or credentials in advance. The objective is to determine what an external attacker could discover and exploit without insider knowledge.

2.1 External Network Penetration Testing

- Identify KLA's internet-facing assets, including any that may be unknown to KLA.
- Assess firewalls, remote-access services, and other externally exposed services at all KLA offices.
- Perform vulnerability scanning, followed by manual validation and, where safe, exploitation of identified weaknesses.
- Determine the extent to which an attacker could gain access to KLA systems or data.

Automated vulnerability scanning alone will not satisfy this requirement. Proposals must clearly distinguish between automated scanning and manual penetration testing activities.

2.2 Public Website

- Assess KLA's public website (www.klaid.org) from an external perspective for exploitable vulnerabilities, misconfigurations, and other security weaknesses.
- Report all identified issues along with recommended corrective actions.

KLA will not provide credentials, source code, or administrative access to the website. Testing must be limited to what can be performed from the public internet and must not disrupt the availability of the website.

2.3 Phishing and Social Engineering

- Conduct at least one simulated phishing campaign directed at KLA staff.
- Report results in aggregate. Individual staff members should not be identified.
- Provide security awareness training recommendations appropriate for KLA's staff and resources.

2.4 Microsoft 365, Identity, and Device Security Review

Certain cloud, identity, device-management, infrastructure, and security configurations cannot be evaluated from outside the organization. Following completion of the black-box testing, KLA will provide the selected firm with read-only access, as appropriate, to review relevant security controls and configurations, including:

- Authentication controls, including multi-factor authentication, passwordless sign-in, conditional access policies, and administrative accounts.
- Device enrollment, configuration, and compliance policies.
- Email security, including anti-spoofing and filtering controls.
- SharePoint and OneDrive sharing settings.
- Audit logging and alerting.
- Backup, recovery, and business-continuity configurations and practices, as appropriate to the selected firm's methodology and KLA's environment.
- Relevant network, firewall, remote-access, and server-security configurations, including the security implications of KLA's ongoing transition away from on-premises systems.

- KLA-controlled security configurations and access-control practices associated with KLA's core platforms, including its case management system, SharePoint environment, Microsoft 365 environment, and cloud-based telephony platform, to the extent permitted by applicable vendor terms.

2.5 Exclusions

The following are outside the scope of this RFP: denial-of-service testing or any activity intended to disrupt services; physical intrusion attempts; and testing of third-party vendor systems, including KLA's case management platform, beyond KLA's own configuration, identity, sharing, access-control, and security settings.

General assessment of KLA's technology-platform selection, staff workflows, user adoption, training, operational procedures, business processes, system usability, reporting practices, or technology-governance practices is also outside the scope of this RFP and is addressed through KLA's separate Technology Assessment. Nothing in this exclusion prevents the security firm from reviewing KLA-controlled security configurations, access controls, sharing settings, identity and authentication controls, device-compliance controls, or other relevant security settings associated with KLA's current platforms.

If KLA's on-premises server has not been retired when testing begins, KLA will notify the selected firm and agree on how it will be addressed.

3. Rules of Engagement

The selected firm must comply with the following requirements:

- No testing may begin until KLA and the firm execute a written authorization identifying targets, dates, testing windows, and emergency contacts.
- The firm must notify KLA immediately of any critical finding or any indication that KLA's systems have already been compromised.
- The firm must not copy, download, or retain client data. If client data is encountered, the firm must stop, document its location, and notify KLA.
- Testing must be conducted to minimize disruption to staff and clients. Any activity likely to affect services requires KLA's prior approval.
- Upon completion of testing, the firm must remove all tools, agents, and test accounts it introduced and confirm their removal in writing.
- All files must be exchanged through a secure method agreed upon by KLA and the firm.
- All findings and evidence must be stored securely during the engagement and securely destroyed at its conclusion, with written confirmation provided to KLA.

4. Required Deliverables

The selected firm will provide the following in editable electronic format and PDF:

1. A kickoff meeting and written testing plan consistent with the rules of engagement.
2. Immediate notification of any critical finding identified during testing.
3. A draft report including an executive summary suitable for KLA leadership; detailed technical findings with risk ratings and supporting evidence; specific remediation steps for each finding; and a prioritized remediation list.
4. A prioritized security remediation roadmap that distinguishes immediate or critical actions from short-term and longer-term recommendations; identifies the relevant system, configuration, policy, or control associated with each recommendation; and provides sufficient detail for KLA to incorporate security priorities into its Technology Improvement Plan.
5. A review meeting with KLA to discuss the draft report.
6. A final report incorporating KLA's feedback and management responses.
7. A summary of the assessment, suitable for sharing with funders, confirming its completion without disclosing sensitive details.

Findings should be provided in a format that allows integration into KLA's Technology Improvement Plan. Proposers should include one coordination meeting with KLA's technology assessment consultant to support integration of security findings with recommendations concerning technology use, staff adoption, training, system integration, reporting, documentation, user support, and governance. The security firm is not expected to conduct or supervise the separate technology assessment.

5. Schedule

The anticipated schedule is:

Activity	Anticipated timing
RFP process, firm selection, and contracting	Nov – Dec 2026
Kickoff and written testing authorization	Jan – Feb 2027
Black-box testing and phishing campaign	March 2027
Microsoft 365, identity, and device review	March 2027
Draft report and review meeting	April 2027
Final report and assessment summary	May 2027
Coordination meeting with technology assessment consultant to share security findings	May 2027

6. Qualifications and Proposal Content

KLA seeks a firm whose primary business includes security assessment and penetration testing. Preferred qualifications include:

- Testing personnel holding recognized penetration testing certifications, such as OSCP, GPEN, PenTest+, or CEH.
- Demonstrated experience assessing Microsoft 365 environments and small, multi-office organizations. Experience with nonprofit or legal services organizations is preferred.
- Demonstrated experience reviewing cloud-based identity, endpoint-management, backup and recovery, remote-access, firewall, server-security, and Microsoft 365 security configurations in small or multi-office organizations.
- Professional liability and cyber liability insurance.

Proposals should include:

1. A cover letter and contact information for the primary point of contact.
2. A brief firm profile and the names, roles, and certifications of personnel who will perform the work.
3. A description of the proposed approach and methodology for each area in Section 2, clearly distinguishing black-box external testing, phishing and social-engineering activities, Microsoft 365 and identity review, endpoint-management review, backup and continuity review, and review of KLA-controlled security configurations for core platforms.
4. A sample report from a comparable engagement, with client information removed.
5. At least three client references for comparable engagements completed within the past three years.
6. A single fixed-fee cost proposal stating the total cost for all work described in this RFP, including travel and any other expenses. Hourly estimates and ongoing subscription or managed-service arrangements will not be considered. Pricing should be based on publicly available information about KLA, and any assumptions made in preparing the cost proposal should be stated.
7. Proof of professional liability and cyber liability insurance.

7. Evaluation and Submission

KLA will evaluate proposals based on responsiveness to this RFP; qualifications and certifications of testing personnel; quality and appropriateness of the proposed methodology; demonstrated experience with external penetration testing, Microsoft 365, identity, endpoint, backup, continuity, infrastructure, and cloud-security review; clarity and usefulness of the sample report; ability to provide practical and prioritized remediation guidance suitable for integration into KLA's Technology Improvement Plan; references; and overall value and cost.

KLA may request interviews, clarifications, additional information, or best-and-final offers and may negotiate scope, deliverables, schedule, and pricing with the selected proposer.

Submit proposals electronically in PDF format by **December 14h, 2026** at **5:00 pm CST** to:

Sarah Hayes
Grants | Pro Bono Director
Kentucky Legal Aid
Email: shayes@klaid.org
Subject line: Security Assessment Proposal

Questions must be submitted in writing to **Rehman Khalid at rkhalid@klaid.org December 7th, 2026**. KLA will share responses to substantive questions with all proposers.

8. General Terms

KLA will not pay costs associated with preparing or submitting a proposal. KLA reserves the right to accept or reject any or all proposals; waive minor irregularities; request clarification or additional information; negotiate with any proposer; modify, suspend, or discontinue this RFP process; or make no award if doing so is in KLA's best interest.

Selection does not create a binding obligation until KLA and the selected firm execute a written agreement. The selected firm will be required to protect the confidentiality of all project information and to comply with applicable confidentiality, data-handling, and conflict-of-interest requirements.

KLA seeks a firm that understands the operating realities of nonprofit civil legal services and will provide rigorous, practical findings that help KLA protect client information and maintain secure, reliable services.