Request for Proposals (RFP)

Technology Assessment and Cybersecurity Audit

Atlanta Legal Aid Society, Inc.
54 Ellis St. NE
Atlanta, GA, 30303

Contact:
Shannon Knox
Director, Information Technology
smknox@atlantalegalaid.org

Introduction and Purpose

Atlanta Legal Aid seeks proposals from qualified cybersecurity firms to conduct a comprehensive Cybersecurity Audit and Risk Assessment of the organization's technology environment.

The purpose of this engagement is to evaluate our current security posture, identify vulnerabilities and risks, and develop a prioritized roadmap for remediation and long-term improvement. The selected vendor will provide independent, expert analysis and actionable recommendations to strengthen protections for sensitive client information, ensure continuity of operations, and support compliance with funder and regulatory requirements.

This RFP outlines the background of our organization, the scope of services requested, the expected deliverables, the evaluation criteria, and the instructions for submitting proposals. Vendors with demonstrated experience in nonprofit, legal services, or similarly complex technology environments are strongly encouraged to apply.

Background

Founded in 1924, Atlanta Legal Aid provides free civil legal services to low-income individuals and families across the Atlanta metropolitan area. With more than 200 staff working from six permanent offices, our attorneys and advocates serve thousands of clients annually in areas such as housing, family law, consumer rights, disability, and public benefits.

Our mission is rooted in protecting the rights and dignity of vulnerable populations—including survivors of domestic violence, tenants facing eviction, and individuals with disabilities. To meet these

responsibilities, we rely heavily on secure and reliable technology systems to safeguard client confidentiality and maintain uninterrupted operations.

Atlanta Legal Aid operates within a hybrid technology environment, which includes:

- Cloud-based platforms: Google Workspace (collaboration), Salesforce (CRM), and LegalServer (case management).
- On-premises infrastructure: Windows Active Directory and Google Workspace Directory for identity management and Meraki firewall-protected local networks across six primary offices connected via a WAN.
- Endpoint environment: A fleet of laptops, desktops, and BYOD mobile devices supporting a distributed workforce of ~150 staff.
- Public-facing assets: A WordPress-based website and related hosted services.

Atlanta Legal Aid recognizes the increasing risks and evolving nature of cyber threats that face nonprofit organizations handling sensitive client information. To ensure the highest standards of data protection and operational continuity, the organization has prioritized strengthening its cybersecurity program. This effort will help safeguard client data, maintain compliance with funder and regulatory requirements, and build a foundation for long-term resilience.

An independent cybersecurity audit will provide the clear, objective baseline needed to understand the organization's current security posture. The findings will guide immediate remediation efforts and inform future strategic technology investments, ensuring that cybersecurity remains integrated into Atlanta Legal Aid's broader mission and operations.

Scope of Work

The selected vendor will conduct a comprehensive Cybersecurity Audit and Risk Assessment of Atlanta Legal Aid's technology environment. The engagement will evaluate technical systems, security practices, and organizational policies to identify vulnerabilities, assess risks, and provide actionable recommendations for remediation and long-term improvement.

The audit will include at a minimum the following areas:

- CIS Cybersecurity Framework Assessment
    - Assess the organization's security posture against the CIS Controls.
    - Identify cybersecurity risks and provide a prioritized roadmap for remediation.
- Compliance & Regulatory Review
    - Evaluate adherence to applicable legal and regulatory requirements, including Legal Services Corporation (LSC) security guidelines.
    - Identify compliance gaps and provide practical recommendations.
- Network Infrastructure Security
    - Review the design, configuration, and security of Meraki firewalls, internal networks, and interoffice connectivity.
    - Assess protection against unauthorized access, misconfiguration, and internal threats.
- Cloud Services and SaaS Security
    - Evaluate security configurations and access controls of Google Workspace, Salesforce (CRM), and LegalServer (case management).

    - Review account permissions, multi-factor authentication (MFA), audit logging, and data-sharing practices.
- Endpoint and Device Management
    - Assess the security of laptops, desktops, and mobile devices, including antivirus coverage, patching/update practices, and remote management capabilities.
    - Identity and Access Management
- Review Windows Active Directory and Google Workspace Directory structure, account lifecycle processes, and privilege management.
    - Assess integration between on-premises and cloud-based identity systems.
- Data Protection and Backup
    - Evaluate data storage locations and backup procedures.
    - Assess readiness against data loss, theft, or ransomware.
- Website and Public-Facing Systems
    - Review the security of the organization's website and other public-facing platforms.
    - Ensure proper patching, monitoring, and hardening against threats such as data exposure or account hijacking.
- Policies and Staff Awareness
    - Review current cybersecurity policies, incident response procedures, and staff training practices.
    - Recommend updates to strengthen the human element of security.
- Testing and Validation
    - Perform vulnerability scanning and penetration testing as appropriate.
    - Validate the effectiveness of current security measures and identify areas of concern.
- Social Engineering Penetration Tests
    - Conduct controlled phishing or related social engineering simulations.
    - Identify vulnerabilities associated with staff awareness and response.
- Data Privacy Assessment
    - Evaluate risks and liabilities associated with data collection, storage, and usage.
    - Provide recommendations to align practices with privacy standards and client confidentiality requirements.
- Disaster Recovery Plan Assessment
    - Review existing disaster recovery and business continuity policies.
    - Provide recommendations for improving documentation, testing, and readiness.
- Documentation Assessment
    - Evaluate current IT and security documentation for completeness, accuracy, and usefulness.
    - Recommend improvements to strengthen institutional knowledge and reduce risk from staff transitions.

Deliverables

The selected vendor will provide the following deliverables as part of the Cybersecurity Audit and Risk Assessment engagement:

- Comprehensive Written Report

    - Executive summary written in plain language for non-technical leadership and Board members.
    - Detailed technical findings for IT staff, including system-specific vulnerabilities, misconfigurations, and risks.
    - Prioritized risk register with severity ratings (e.g., critical, high, medium, low).
    - Recommendations for both immediate remediation and long-term security improvements.
    - Assessment results mapped to CIS Controls framework.
- Presentation and Q&A Session
    - Formal presentation of findings to organizational leadership and IT staff.
    - Dedicated time for discussion, clarification, and Q&A.
    - Optional session tailored for the Board of Directors, if requested.
- Remediation Roadmap
    - Clear, prioritized roadmap for addressing identified risks.
    - Suggested sequencing of remediation steps based on risk level, resource requirements, and operational impact.
    - Guidance on policies, procedures, and staff awareness initiatives.
- Supporting Materials
    - Documentation of all testing performed, including vulnerability scans, penetration testing results, and social engineering assessments.
    - Compliance gap analysis with specific reference to LSC security guidelines and other relevant regulations.
    - Recommendations for improving IT/security documentation and disaster recovery plans.
- Knowledge Transfer
    - Direct consultation with Atlanta Legal Aid's IT team to explain findings and ensure understanding of remediation steps.
    - Provision of sample templates or reference materials (e.g., policy outlines, checklists) where applicable.

Timeline

Procurement Phase

- RFP Issued: October 15, 2025
- Vendor Questions Due: October 31, 2025
- Responses to Questions Provided: November 7, 2025
- Proposal Submission Deadline: November 21, 2025
- Vendor Interviews (if applicable): December 8 – 12, 2025
- Contract Negotiation and Execution: January 16, 2026

Project Phase

Project Start Date: February 2, 2026

- Phase 1: Planning and Engagement (Months 1–3)
    - Finalize scope, audit schedule, and data access requirements.

    - Conduct kickoff meeting with organizational leadership and IT team.
    - Develop communication protocols to minimize disruption during the audit.
- Phase 2: Cybersecurity Assessment and Testing (Months 3–5)
    - Perform comprehensive audit of technology environment, including:
    - Network infrastructure security review.
    - Cloud and SaaS platform configuration analysis.
    - Website and hosting security review.
    - Endpoint/device management evaluation.
    - User authentication and Active Directory assessment.
    - Backup and disaster recovery readiness.
    - Vulnerability scans and penetration testing.
    - Conduct staff input sessions or security culture assessments, as appropriate.
- Phase 3: Analysis and Recommendations (Month 6)
    - Compile findings into a comprehensive report.
    - Provide prioritized list of vulnerabilities, risks, and recommendations.
    - Present results to Atlanta Legal Aid leadership and IT team, including discussion of recommended remediation roadmap.
- Phase 4: Follow-Up and Remediation Planning (Months 7–9)
    - Support immediate remediation of critical findings (e.g., patching, MFA enforcement, policy updates).
    - Assist in developing updated cybersecurity policies and procedures.
    - Provide guidance on longer-term initiatives such as staff training, infrastructure upgrades, and technology planning.
    - Conduct a final debriefing with leadership to align cybersecurity roadmap with organizational strategy.
- Ongoing (Post-Engagement)
    - Findings may be used to inform future funding applications and strategic planning.
    - Vendor may be considered for follow-up engagements, subject to performance and organizational needs.

Evaluation Criteria

Relevant Experience and Qualifications (25%)

- Demonstrated experience conducting cybersecurity audits and risk assessments for organizations of similar size and complexity.
- Experience working with nonprofit, legal services, or other mission-driven organizations.
- Qualifications, certifications, and expertise of proposed project team members.

Approach and Methodology (25%)

- Clarity, feasibility, and completeness of the proposed approach to the audit.
- Alignment of methodology with the scope of work outlined in this RFP.
- Incorporation of recognized cybersecurity frameworks, standards, or best practices (e.g., CIS, NIST, ISO).

Deliverables and Reporting (20%)

- Quality and usefulness of proposed deliverables, including final reports, risk assessments, and remediation roadmaps.
- Commitment to knowledge transfer and actionable recommendations that support Atlanta Legal Aid's long-term cybersecurity maturity.

Cost Proposal (20%)

- Overall cost-effectiveness and clarity of pricing structure.
- Transparency regarding fees, expenses, and potential additional costs.
- Alignment of proposed budget with organizational resources.

References and Past Performance (10%)

- Strength of references from comparable clients.
- Evidence of successful project outcomes and client satisfaction.

Proposal Submission Instructions

Proposals must include the following components:

- Cover Letter – Brief introduction of the firm, including an authorized point of contact.
- Company Profile – Background on the organization, including size, areas of expertise, and relevant certifications.
- Experience and Qualifications – Description of relevant engagements, particularly for nonprofit or legal services organizations, and bios of key personnel.
- Proposed Approach and Methodology – Detailed description of how the firm will conduct the audit, including tools, techniques, and frameworks.
- Deliverables – Outline of specific deliverables that will be provided, including reports, presentations, and recommendations.
- Timeline – Proposed project schedule, including milestones and dependencies.
- Cost Proposal – Itemized pricing, including professional fees, travel, and any other anticipated expenses.
- References – At least three client references for similar work performed within the past five years.

Proposals must be submitted electronically in PDF format.

Questions

- All questions regarding this RFP must be submitted in writing by October 31, 2025 to smknox@atlantalegalaid.org.
- Responses to questions will be distributed to all potential bidders to ensure fairness and transparency.

All submissions should be directed to:

Shannon Knox
Director of Information Technology

Atlanta Legal Aid
Email: smknox@atlantalegalaid.org

Deadline

- Proposals must be received no later than November 21, 2025.
- Late submissions may not be considered.