Request for Proposal - Cybersecurity Risk Assessment

Issued by: Michigan Advocacy Program
Due Date: 10/31/2025
Submit to: Amanda Revels
Chief Operating Officer
arevels@lsscm.org

1. About Michigan Advocacy Program

Michigan Advocacy Program (MAP)'s mission is to advance the safety, independence, and economic stability of those most affected by poverty, racism, and other structurally oppressive systems by increasing access to justice and working for systemic solutions. MAP's direct services components are: 1) Legal Services of South Central Michigan, which provides free civil legal advice and representation to low-income residents of 13 counties in south central Michigan and 2) Farmworker Legal Services, which provides free legal assistance to migrant and seasonal farmworkers throughout the State of Michigan. MAP also provides administrative services to the five statewide programs of Michigan Statewide Advocacy Services, including the Michigan Poverty Law Program, Michigan Legal Help, the Michigan Immigrant Rights Center, the Michigan Elder Justice Initiative, and the Crime Victims Legal Assistance Project.

MAP is a grantee of Legal Services Corporation and must adhere to compliance requirements for information technology and cybersecurity listed in the LSC Financial Guide. At a minimum, risk assessment procedures should provide the following:

- Identify the physical and digital assets susceptible to cyberattacks
- Identify risks to those assets (risks should be evaluated annually for changes)
- Evaluate the risks (e.g., high, medium, or low) based on likelihood and impact
- Document the results of the risk assessment, including the development and implementation of appropriate controls

2. Purpose of the RFP

The purpose of this Request for Proposal (RFP) is to identify and select a qualified, experienced cybersecurity firm to assist our non-profit legal aid organization in enhancing the security and resilience of our information systems and data protection practices.

We seek a cybersecurity partner to perform a comprehensive assessment of our current cybersecurity posture, including technical infrastructure, organizational policies, and user practices. This engagement will include:

- Identification of vulnerabilities and threats across our IT environment, including network security, data storage, access controls, and end-user behavior;

- Evaluation of compliance with relevant legal, ethical, and regulatory standards, such as the American Bar Association (ABA) cybersecurity guidance, the Health Insurance Portability and Accountability Act (HIPAA), state-specific privacy and data breach notification laws, and other applicable frameworks;
- Delivery of actionable recommendations for mitigating risks, improving controls, enhancing user awareness, and strengthening incident response and data protection protocols;
- Support for our ongoing commitment to safeguarding client confidentiality, minimizing risk exposure, and ensuring trust among our clients, funders, partners, and community stakeholders.

3. Scope of Work

The selected vendor will be expected to:

1. **Review IT Infrastructure & Policies**
    - Conduct a complete analysis of network architecture, including firewalls, switches, routers, and wireless access points.
    - Review servers, workstations, laptops, and mobile devices for configuration, lifecycle management, and security controls.
    - Assess use of cloud services and hosted applications, evaluating integration, data security, and redundancy.
    - Review and evaluate existing IT and cybersecurity policies, procedures, and incident response plans to ensure alignment with best practices, legal requirements, and organizational needs.
2. **Perform a Risk & Vulnerability Assessment**
    - Perform internal and external penetration testing to identify exploitable weaknesses.
    - Conduct automated and manual vulnerability scans across systems, networks, and applications.
    - Review third-party vendor risk to identify and assess potential threats that may arise from engaging outside parties for goods or services; such as vendors, contractors and suppliers.
    - Identify risks related to social engineering, phishing, and other human-factor vulnerabilities.
    - Evaluate the effectiveness of current monitoring and intrusion detection/prevention systems.
3. **Review Data Security & Compliance**
    - Assess encryption practices for data at rest and in transit.

- Evaluate user access controls, identity management, and authentication methods.
- Review data retention, backup, and recovery policies and procedures.
- Determine compliance with applicable regulations (e.g., HIPAA, ABA guidance, state data privacy laws) and ethical obligations specific to legal practices.

4. **Evaluate Staff Awareness**

    - Review user account provisioning, deprovisioning, and access management procedures.
    - Assess existing staff training programs, security awareness initiatives, and phishing simulations.
    - Provide recommendations for strengthening user accountability and organizational culture of security.

5. **Prepare & Present a Comprehensive Report with Recommendations**

    - Deliver a detailed written report summarizing findings, risk ratings, and prioritized recommendations.
    - Provide practical, cost-effective solutions tailored to the organization's mission, size, and resources.
    - Present results to leadership and/or the Board of Directors, including executive-level summaries and technical appendices as appropriate.

6. **Propose Ongoing Support**

    - Vendors may include proposals for ongoing support, which may include retainer services, periodic vulnerability scans, follow-up assessments, or training refreshers.
    - Optional support should be clearly itemized with associated costs, service levels, and response times.

4. Minimum Deliverables

- Executive summary for leadership
    - Plain-language overview of the organization's current cybersecurity posture.
    - Key vulnerabilities and risks explained in non-technical terms.
    - Prioritized recommendations for resource allocation and decision-making.

- Detailed technical report with vulnerability findings
    - Comprehensive review of network, endpoint, access controls, and data protection measures.
    - Results from vulnerability scans, penetration testing (if in scope), and configuration reviews.

    - Identification of weaknesses such as outdated software, weak authentication, or insufficient encryption.
    - Technical detail sufficient for IT staff or outside vendors to take corrective action.

- Risk matrix with severity levels
    - Categorization of risks by likelihood and impact (e.g., low, medium, high, critical).
    - Visual matrix to quickly show priority areas.
    - Helps leadership and IT teams align on which risks demand immediate attention.

- Roadmap for remediation
    - Categorize recommendations into short-term “quick wins” (e.g., enabling MFA, updating patches, strengthening password policy), medium-term initiatives (e.g., upgrading firewalls, improving backup processes, implementing endpoint detection) and long-term strategies (e.g., zero trust architecture, vendor risk management, staff phishing simulations).
    - Clear assignment of responsibility and proposed timelines.
    - Cost estimates or resource implications where possible.

- Debrief Presentation
        - Presentation to leadership or designated stakeholders Live or virtual briefing summarizing the assessment’s findings and recommendations tailored to non-technical leaders such as the Executive Director, Board of Directors, or senior program managers.
    - Presentation to IT personnel
        - Live or virtual briefing tailored for IT staff summarizing the assessment’s findings and recommendations.
            - Configuration changes, patching requirements, and system hardening steps for IT staff
            - Incident response and monitoring recommendations for IT staff

5. Timeline

Task	Date
RFP Issued	10/6/2025
Questions Due	10/24/2025
Proposals Due	10/31/2025
Vendor Selection	11/30/2025
Project Kickoff	12/15/2025
Final Report Delivered	3/31/2026

6. Proposal Requirements

Vendors must include:

1. **Company Overview –** history, size, location(s), and relevant certifications (e.g., CISSP, CISM, CEH).
2. **Experience –** similar engagements with non-profits, LSC grantees, legal organizations, or entities handling sensitive client data.
3. **Project Approach & Methodology –** detailed process for performing the assessment.
4. **Team Qualifications –** names, titles, certifications, and relevant experience.
5. **References –** at least three organizations served in the last three years.
6. **Cost Proposal** – breakdown by phase or deliverable, including any optional services. The proposal must include the fee proposal for the goods and/or services along with a proposed schedule of payments, proposed project schedule, and timeline. MAP will not pay any vendor costs associated with preparing responses submitted in response to this RFP.
7. **Insurance & Security Compliance –** proof of professional liability and cyber liability insurance.

7. Evaluation Criteria

Proposals will be evaluated based on:

- Vendor's relevant experience and qualifications - demonstrated expertise in performing cybersecurity assessments, particularly for non-profits, legal organizations, or LSC grantees; qualifications and certifications of key personnel (e.g., CISSP, CISM, CEH, GIAC, CISA)
    - The vendor must demonstrate knowledge of Microsoft Intune compliance policies for mobile device management (MDM) of company-owned and personally-owned devices, as well as, mobile application management (MAM) of guest user access to SharePoint online.
    - The vendor must demonstrate knowledge of Google Workspace for email, calendar, browser security, SAML single-sign-on, etc.
    - The vendor must demonstrate knowledge of Salesforce security best practices.
    - The vendor must demonstrate knowledge of Unifi networking devices.
- Understanding of scope and proposed methodology - demonstrated understanding of the objectives and requirements outlined in this RF including consideration of LSC's cybersecurity requirements, and innovation in ability to balance technical rigor with non-profit resource constraints.

- Cost - overall cost-effectiveness of the proposal, including total fees and value provided and transparency of pricing structure, with clear breakdown by phase, deliverable, or optional services.
- References - evidence of successful completion of similar engagements within the last three years and ability to deliver on time and within budget.
- Proposed timeline and deliverables - realism and practicality of the proposed project schedule and clarity and completeness of proposed deliverables, including tailoring for both executive leadership and technical staff.

8. Submission Instructions

- **Format:** PDF preferred
- **Delivery Method:** Email to Amanda Revels, Chief Operating Officer, arevels@lsscm.org by 10/31/2025
- **Subject Line:** "Cybersecurity Risk Assessment RFP – [Your Organization Name]"
- **Deadline:** 10/31/2025

Late submissions and submissions over 10 pages will not be considered.

9. Questions

All proposals must be submitted electronically in PDF format to arevels@lsscm.org no later than 10/31/25.

For questions, contact Amanda Revels at arevels@lsscm.org.

10. Confidentiality & Disclaimers

- All information provided to the selected vendor will be considered confidential and subject to applicable privilege and privacy laws.
- MAP reserves the right to change the RFP Schedule or issue amendments to this RFP at any time. MAP also reserves the right to cancel or reissue the RFP.
- MAP reserves the right to enter into contracts with more than one vendor as a result of this RFP.
- Any products, deliverables, data, and other shall be owned by MAP
- All responses, accompanying documentation and other materials submitted in response to this RFP, or in response for more information, shall become the property of MAP and will not be returned.
- The vendor chosen will be asked to sign a non-disclosure agreement affirming the confidentiality of MAP's content and other aspects of the project.