



# GOGEBIC-ONTONAGON COMMUNITY ACTION AGENCY

100 S. Mill St., Bessemer, MI 49911

Phone: (906) 667-0283 Fax: (906) 663-0356

TTY Voice Mail: (800) 649-3777



March 3, 2020

## Request for Quotations for Cybersecurity Services

### I. Purpose / Scope

Gogebic Ontonagon Community Action Agency, (GOCAA), is issuing this Request for Proposal (RFP) to select a firm to conduct independent audit and testing services for the GOCAA's cybersecurity program and controls.

### II. Corporate Profile

GOCAA is a 501 c 3 non-profit corporation whose mission is to reduce poverty in Gogebic and Ontonagon Counties. GOCAA has several locations of service in our two-county area.

### III. Requirements

GOCAA is requesting a proposal to complete the cybersecurity audit, testing, and assessment to evaluate the organization's overall security program to ensure we meet industry best-practices, and regulatory requirements for data protection. GOCAA is also requesting assistance in fixing cybersecurity vulnerabilities. Please clearly respond to how your firm will address the following requirements:

#### Requirement 1: Cybersecurity Program Health Check

Assess the overall maturity of GOCAA's cybersecurity program, identify areas for improvement and create a risk remediation roadmap. We would like to have the cybersecurity program to be evaluated against controls categories provided by a recognized authoritative source, such as NIST. We control categories should include but not limited to:

<ul style="list-style-type: none"> <li>• Security Culture and Governance</li> <li>• Training and Awareness</li> <li>• Vulnerability Management</li> <li>• Identify and Access Management</li> <li>• Business Continuity</li> <li>• Data Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Response</li> <li>• Third Party Risk</li> <li>• Physical Security</li> <li>• Human Resources Security</li> <li>• Technical Controls</li> </ul>
---	--

### **Requirement 2: Vulnerability Assessment**

GOCAA would like to validate the effectiveness of key technical controls that safeguard the organization's sensitive data including (but not limited to):

1. Internet perimeter security assessment
2. Internal network security vulnerability scanning

### **Requirement 3: Social Engineering – Email phishing**

To assess internal cybersecurity awareness of employees, we would like vendor to propose conducting an email phishing attempt that targets up to 50 employees.

### **Requirement 4: Employee Security Awareness Training**

Quarterly online security training to improve the culture of employee awareness with ability to track progress and participation..

### **Desired Deliverables**

Assessment reports for each project including:

- Cybersecurity program assessment with maturity ratings and prioritized and actionable recommendations.
- Comprehensive assessment of technical (internal and external) vulnerabilities.
- Assessment of internal security awareness culture through email phishing.
- Remediation roadmap that includes budget estimates, timeline, and level of effort
- Presentation to Management or Board of Directors

### **Scoping information:**

- Number of locations: 6
- Number of employees: 70-90
- Total number of active external IP addresses: unknown
- Estimated number of internal IP addresses: unknown

- Number of Servers (including virtual) by operating system
- Number network devices (routers, switches, firewalls, etc.)
- Workstations / laptops:
- Overview of WAN topology Unknown
- Number of cloud service providers (e.g. Office 365, Azure, AWS) Unknown

### **Information Requested**

Please include the following within your response to assist with our selection:

- Statement of work and fees for each project including fees
- Experience / Background providing the services requested
- Certifications of Personnel
- Identify if vendor will use sub-contractors or employees
- References
- Information on vendor's financial stability
- Insurance

### **RFP Terms and Conditions**

- Clarification Process – Questions about this Request for Proposal may be directed to the Executive Director at 906-667-0283 ext. 8 or by USPS mail at the above address
- Response format and deadline – Mail responses to GOCAA at the above address. Deadline for Proposal: **Noon, March 25<sup>th</sup>**
  - Executive Summary
  - Statement of Work
  - Pricing
  - Assumptions
  - Required Responses (see "Information to Request")
- Evaluation process
  - Decision on vendor selection will be made by March 31, 2020
  - Work to begin as early as April 1, 2020 and end no later than September 15, 2020
  - GOCAA uses a standard procurement scoring form and has the right to accept or reject any bid.