

**NEW MEXICO PUBLIC SCHOOLS INSURANCE AUTHORITY**

**REQUEST FOR PROPOSALS (RFP)**

**Cyber Security Risk Assessment and Consulting Services  
Amendment #1**



**RFP# 342-2022-03**

**RFP Release Date: April 26, 2022**

**Due Date: May 16, 2022**

**ELECTRONIC-ONLY PROPOSAL SUBMISSION**

## IV. SPECIFICATIONS

### A. DETAILED SCOPE OF WORK

**THE TERM** or length of engagement will be approximately ~~four (4) to eight (8) weeks.~~ **One (1) year.**

The resulting contract will be a single award. This procurement will result in a contractual agreement between two parties; the procurement may ONLY be used by those two parties exclusively.

The Authority is soliciting proposals from highly qualified Contractors who will conduct cyber security assessments and provide risk mitigation recommendations for the K-12 School Districts (88), postsecondary education institutions (7), charter schools (99), and other supporting education entities (11) as members to the Pool. The firm selected will perform a cyber security risk-related assessment for each of the 205 members of the Pool as they are listed on Exhibit A and any new members that may be added under the contract term under the Detailed Scope of Work. The assessment requires a firm's capability to administer an external network scan of members systems by using data - driven, objective and available public metrics to evaluate networks' susceptibility to risks. The security assessment must include an evaluation of members' IT infrastructure to identify and quantify potential network vulnerabilities involving, but not limited to, configurations of email security, detection of malware actions, patching cadence, back up, certificates, domains, out of dates services and other critical risk vectors targeted to compromise network systems and applications used by Authority members.

Proposals shall state whether your firm can provide a service with the following features and state if the firm is not so capable and if not, why the firm believes the feature may not be necessary to the Authority program. Minimum services to be performed are outlined below.

- Perform an external vulnerability scan of network systems for each Pool member. It shall be each member's responsibility to provide Contractor their own domain information for its organization in a timely manner.
- Provide an overview report in XML and PDF format affording an objective risk evidence-based assessment of each member's cyber risk and overall security preparedness. The criteria of the report will be standardized. Each Authority member shall receive a report on its own network.
- Provide a single software system that provides member access via requiring logins to a password-protected, internet-based interface to access reports. The software program should serve both the monitoring and administration function of its members and must have a dashboard that is user-friendly that quickly allows each member designated representatives to access and review its own network evaluation metrics and reporting.

- Review each member's current procedures and practices versus acknowledged best practices and make and implement recommendations or remediation strategies to enhance member's cybersecurity program.
- Provide network monitoring and technical support services on the use of any software and be available between 8:00 AM to 5:00 PM MST for assistance to member representatives to include, but not limited to, exchange and retrieval of network data, interpreting assessment results and analytics, guidance for remediation practices and software support.

The Contractor shall act as the Authority's representative to all Authority members and employees with respect to Cyber Security Risk Assessment Services for the Authority. The Contractor must meet all applicable State and Federal regulations and laws applicable to the program and the work to be performed. Any additional services, or services which the Contractor cannot perform, must be outlined in the written proposal. **In addition, the Contractor shall submit a detailed work plan showing timelines for completion of the work.**

The Contractor shall provide all labor, materials, equipment, and supervision to provide Cyber Security Risk Assessment and Consulting Services.