**Request for Qualifications**

**NC FY21 - Combatting Domestic Violence Extremism Project**

***Introduction***

The North Central Regional Planning Commission, located at 109 N. Mill St. Beloit, Kansas 67420, is the fiscal agent for and behalf of the North Central Regional Homeland Security Council. The Council is seeking a Consultant capable of developing a set of documents (i.e., Extensive written report based on the results of a Penetration Test, Policies, and Procedures) that identify gaps and enhance a county's Cybersecurity program. The North Central Region would like to provide this service to the region in a phased approach, starting with one county. This will be an ongoing project for the North Central Region. This portion of the project will be funded through FY21 Federal Homeland Security program funds. This project must be completed no later than May 31, 2023.

The project committee for this North Central Homeland Security project is comprised of individuals who are actively involved in providing cybersecurity to the county government and knowledgeable of the activities and actions that would need to be taken in the event of a cybersecurity incident. These individuals are appointed to the Council by their respective member governments, disciplines, and/or organizations. They are seen to reflect the disciplinary concerns and interests of all those who hold similar positions throughout the North Central Region.

The North Central Regional Planning Commission thus invites all interested parties to submit written statements of qualifications pertaining to the following.

***Project Goal***

The principal goal is to create and enhance cybersecurity programs in each county government within the North Central Region. This will involve any initial examination of the preexisting system, which a Penetration Test will do. The Penetration Test results will then be compiled into an extensive written report to include gaps and suggested mitigation strategies to rectify those identified gaps and presented to the County. The County will then take the proposed mitigation actions. A retest of the one previously performed on the system will be done to examine the success of the mitigation efforts. The Consultant will be asked to provide the County with a schedule, checklists, and policies and procedures to raise the level of the County's Cybersecurity program.

***Geography Involved***

This project addressed the cybersecurity needs of the North Central Homeland Security Region. This project will also serve as the pilot cybersecurity program for the State of Kansas.



The North Central Regional Homeland Security Council serves twelve (12) counties. It is composed of individuals who are representative of the agencies and organizations that respond to cyber-related emergencies within the following counties:

Smith Jewell Republic

Osborne Mitchell Cloud

Clay Lincoln Ottawa

Ellsworth Saline Dickinson

***Project Committee***

The Project Committee is comprised of 4 representatives that are responsible for responding to cyber-related emergencies. The Committee was created to ensure the project aligns with the overall desired outcome for this project. The Project Committee will develop the standards and guidelines for selecting a Consultant. However, once that selection is made, the vendor will work directly with the County. The Project Committee will oversee the entire project to ensure that the project goals and anticipated products are developed while the timeline is kept. There will be no sensitive information specific to the County shared with the Project Committee.

***Selection Criteria and Interview Process***

The Project Committee will review all submitted qualification statements and select no less than three (3) Consultants to interview based on the following criteria.

1. Consultants will provide a list of systems they have experience with, including Enterprise applications that they are comfortable working on.
2. Consultants will provide work samples of written reports for both deliverables.
3. Consultants must have experience in either providing similar services to another customer or experience in fixing or evaluating the aftermath of an intrusion.
4. Evidence of adequate staff capacity and capability to perform the desired tasks – penetration testing may either be done by the Consultant or subcontracted out.
5. Provide an example of what a vulnerability assessment means to your company and what you would do when providing one.
6. Consultants must be knowledgeable in CIS Standards.
7. Consultants must provide a list of references that they have provided services.

The interview process for *each* interview will last no more than one (1) hour. The Project Committee will expect the Consultant to provide greater detail as to background experience and engage in a question and answer session concerning the overall scope of the project and the anticipated process and outcome desired. Consultants will be encouraged to challenge the Committee on its thinking and offer any suggestions the Consultants might have concerning the project.

Following the interviews, the Project Committee will rank the Consultants interviewed, then make arrangements to negotiate the terms of a final agreement with the highest-ranked Consultant. If an agreement is reached, the North Central Regional Planning Commission will develop a contract. If no agreement is achieved with the Consultant, the Project Committee will repeat the process initiating similar contract negotiations with the second-highest ranked Consultant.

***Budget and Contract***

The North Central Regional Planning Commission, as a fiscal agent to the North Central Homeland Security Council, will enter into a contract with the selected consulting firm. However, be informed that the Kansas Highway Patrol must approve the contract document before the final execution of the contract. The North Central Regional Planning Commission will require a time and expense agreement as part of the contract with an established not-to-exceed maximum fee to provide maximum flexibility.

***Scope of Work***

The anticipated process will include, at a minimum, the following sequential steps, which are spelled out in greater detail below.

*Task 1: Penetration Test*

For this project's scope, Penetration testing is defined as security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. The Consultant will offer the County the option to select the internal and external Penetration Testing they wish to participate in that is applicable for the County's environment. The three (3) options will include Black Box, Gray Box, and White Box Penetration Testing.

1. White Box will be defined as a test methodology that assumes explicit and substantial knowledge of the assessment object's internal structure and implementation detail.
2. Gray Box will be defined as a test methodology that assumes some knowledge of the assessment object's internal structure and implementation detail.
3. Black Box will be defined as a test methodology that assumes no knowledge of the assessment object's internal structure and implementation detail.

*Task 2: Penetration Results Report*

The Penetration test will be followed up with an extensive written report of the penetration test findings - to include cybersecurity gaps, suggestions for mitigation and remedies for gaps, and additional hardware and software that would rectify the identified gaps for the county. The report will be submitted to the respective County's point of contact and asked to present the findings to the County Commission. Depending on the sensitivity of the information, this will be done in either a public open meeting or study session (exempt from the Open Records Act).

*Task 3: Retest*

Within 90 days of the mitigation and remedies being implemented, the Consultant will conduct an exact retest to the one previously performed on the respective County and provide a comprehensive analysis of the new test results to determine if the previous mitigation and remedy recommendations were successful and effective.

*Task 4: Vulnerability Assessment*

For the scope of this project, Vulnerability Assessment is defined as a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. The Vulnerabilities Assessment will involve a review of the hardware and software configurations, which must be utilized to establish the Cybersecurity Program for the County.

*Task 5: Maintaining the County's Cybersecurity Program*

The Consultant will work with the county to establish a Cybersecurity Program. This program will consist of establishing schedules, checklists, and policies and procedures to maintain the integrity of the County's Cybersecurity. These tools will be utilized to monitor and define the performance of the County's I.T. Department or County's I.T. Consultant. The program must consist of the following areas, but is not limited to, O.S. and software patches, antivirus, and device firmware updates. The program is to include general cybersecurity and system-specific recommendations.

***Directions for Submission of Qualification Statements***

Interested individuals, firms and/or organizations are to submit one (1) hard copy of their Request for Qualifications proposal to the following address:

 Lisa Peters

North Central Regional Planning Commission

109 N MIll Street, PO Box 565

Beloit, KS 67420

Such proposals must show the respondent holds appropriate qualifications and/or credentials reflecting the services needed; illustrate they have provided services similar to those specified herin; and, at a minimum, include the following information.

1. Consultant name and address.
2. Brief history of operation and range of service capabilities.
3. Name and resume of Project Director.
4. Resumes of all principals and professional support staff involved, demonstrating qualifications and related experience and expertise.
5. No less than three (3) references, including contact information and a brief description of the project service(s) provided.
6. Proposed cost for all services to be delivered.

**Deadline: 10:00 am, Friday February 24, 2023**