

Addendum I For RFP #19-04

For Network Security & Risk Assessment

In response to questions provided by vendors, Greenville Utilities Commission (GUC) is providing the following information as an addendum to our RFP. If a vendor's specific question is not addressed in the information below, GUC does not believe that information is appropriate to provide at this stage of the RFP process.

Background information

GUC has 465 employees working from 6 campuses and in the field, all of which are in Pitt County, NC. There are approximately 500 workstations, 250 servers and 90 switches and routers, as well as multiple mobile devices, including laptops, tablets, and smart phones. We have a primary data center and two auxiliary data centers. We maintain several wireless networks for use by employees, contractors and guests across all 6 locations as well as at a few substations. From time to time employees, contractors and vendors utilize a VPN to establish a secure connection from their remote location to our network.

GUC's enterprise systems are currently supported by 3 different relational database management systems, two operating systems and a cloud-based email system. GUC does make use of virtualization at the server level with two hypervisors. An imaging system, a security camera system, access cards and Voice over IP are all being used in our environment.

GUC deploys several security mechanisms used in the defense of its information systems, including firewalls, Intrusion Prevention Systems and end-point security applications. GUC also operates a cyber security awareness training program that is mandatory for all employees. The vendor should assess current network security capabilities and their ability to identify and potentially stop cyber-attacks, data loss, and misuse of IT resources.

Policies

The selected vendor is expected to review for gaps in and make recommendations on GUC's Security Policies & Governance Documents. GUC has several formal written policies that will be available for the selected vendor to review, totaling approximately 80 pages. It is expected the selected vendor will consider general practices and processes as part of the overall assessment, some of which might be undocumented. We expect that GUC personnel needed for the assessment will be made available for discussions as needed.

Scanning and Testing

Based on the RFP provided, we expect scanning to be executed only as necessary to establish the overall security posture and risk level of the commission. If the assessment needs to include vulnerability or penetration testing, or social engineering, we can discuss specific scope after the selection of a partner. We would expect any scans, tests, etc. to be non-disruptive to business and field operations.

Physical Security

We consider an overall assessment of physical security policies and practices a factor in overall security posture, however, we do not consider any sort of interactive tests of those measures to be in scope.

Configuration Review

Once a vendor is selected, we will provide sample workstations, laptops, etc. for review. The selected vendor will be authorized to review configuration of devices on corporate and SCADA networks as necessary. We expect that GUC personnel needed for the assessment will be made available for discussions as needed.

Cost

This project requires a not to exceed bid amount to complete the assignment and the cost shall be all inclusive of travel expenses and other incidental costs associated with the project. Costs and expenses relating to the preparation of a proposal and its submission are to be borne solely by the Vendor. Please provide the following:

1. **Single hourly rate** which will apply to all work efforts, regardless of type or complexity. Also, it will apply to all Vendor personnel, regardless of required skill or experience levels. The single hourly rate will cover all costs, including direct and overhead expenses. Travel, per diem and other miscellaneous costs will be absorbed in the single rate. (This supersedes item 6 at the top of page 4 of the RFP; rates for each classification of personnel is not required.)
2. **Number of Hours to Complete Major Project Sections.** Provide a sub total of the hours allocated to each major section of your proposal, e.g. Discovery, Policy review, Scanning, Personnel interviewing, Write up, etc.
3. **Number of Hours to Complete the Project.** This should be the sum of the hours provided for individual sub sections as broken down in the Timetable/Schedule below.
4. **Assessment Category** GUC believes this assessment is classified as a Medium assessment. Vendor must indicate whether this project would be categorized as a small, medium or large assessment based on the requirements stated herein.

Timetable/Schedule

The vendor must provide a timetable for completion for the security assessment requested in the RFP, with a break down by major sections of work. Vendor must show the number of hours required to complete each section and the total project. The assessment must begin within two weeks after the RFP is awarded.

General Expectations & Clarification

This assessment is expected to focus primarily on overall risk, especially as a function of governance and policy. We do not expect phishing, scanning of web applications, databases, wireless networks and operating systems to be the primary task associated with this exercise, and should be done only as necessary to support the overall risk assessment.

GUC's goal is to utilize this assessment to identify deficiencies in its security program—especially regarding policy, governance, and structure. All deliverables from this assessment should serve to create a priority list and roadmap for remediation.

Miscellaneous

The vendor will provide a reciprocal non-disclosure agreement for the benefit of both parties.

PROPOSALS SHALL BE RECEIVED BY 3:00 PM (EDST) ON February 11, 2019.

Proposals shall be submitted to Cleve Haddock, CLGPO, Procurement Coordinator, Greenville Utilities Commission, 401 S. Greene Street, Greenville, North Carolina 27834. GUC reserves the right to reject any and all Proposals.