Greenville Utilities Commission

Questions and Answers II for #17-09

RFQ For Assessment And Penetration Services, 2/9/17

1 In your answer to number three, you mentioned placing a compromised machine on your network. In the interest of minimizing the costs associated with the testing, travel, etc. are you open to us sending you our testing system so that all work can be done offsite? Note that we can provide GUC staff access to the system to show that it is up to date on patches, and running antivirus, etc. Please provide clarification.

GUC would be willing to a place a pre-configured machine on our network so long as that machine is only used for purposes of this penetration test.

2. Please let me know if you need clarification on the application testing piece – application size information is very helpful for pricing. For instance, it's good to know whether to price it like a large SAP portal or a e-shopping cart.

From the RFQ, we expect you to exploit known vulnerabilities on Oracle enterprise systems. We consider Oracle systems to be SAP like in size.

3. Agio's policy is to not accept terms that do not include a limit of liability. Can Greenville Utilities accept some reasonable limitation of liability and add that to the terms?

This question will be recorded and addressed by legal at a later date.

4. <u>SCADA Testing Questions -</u>

ESPs (Electronic Security Perimeters): This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many separate electronic security perimeters are in scope (separate networks containing Critical Cyber Assets): This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many live IPs are externally accessible across all ESPs: This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many infrastructure devices are in scope across all ESPs (firewalls, routers and switches that define/control the ESPs): This information would disclose specifics about our system architecture. We will disclose this information later in the process.

Firewalls:
Routers:
Switches:

How many Critical Cyber Assets reside within all ESPs: This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many non-critical devices reside within all ESPs: This information would disclose specifics about our system architecture. We will disclose this information later in the process.

PSPs (Physical Security Perimeters): N/A
How many separate physical security perimeters are in scope (separate offices/datarooms/cages containing Critical Cyber Assets): N/A
How many physical security systems are in scope across all PSPs (servers, end point security systems): N/A

Substations (in scope by 2015 with CIP v5): This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many substations in the organization: This information would disclose specifics about our system architecture. We will disclose this information later in the process.
How many of each below across all substations: This information would disclose specifics about our system architecture. We will disclose this information later in the process.

Firewalls:
Routers:
Switches:
Servers (EMS, SCADA, …):
HMIs:
RTUs (2032s…):

5. Application Testing Questions -

Are you interested in in-depth application testing with credentials? NO
Number of in-scope, externally or internally accessible applications/sites: N/A

Please answer the following for each application
How many "pages" with interactive inputs to test? (Please describe pages): N/A
How many unique user roles: N/A
Which technologies / platforms / languages are being used? N/A
What does the app do? N/A

6. Other Questions-

Is this assessment for compliance? (Y/N - If yes list the standard or regulation below) N
Are you interested in pricing on a Black Box Penetration Testing (capture-the-flag exercise)? N

Perimeter Security Assessment/ External Penetration Testing Questions

Number of locations with Internet facing networks:
Number of in-scope, externally addressable systems (live IPs) across all locations: 0
Number of in-scope, externally accessible web applications/sites: 0

Do you have an Intrusion Prevention System (IPS)? Y
If yes, would you like differential testing (with and then without whitelising)? N

Internal Pen Testing Questions

Are you interested in an internal security assessment? (Y/N - If yes, please answer the questions below) Y
Number of in-scope locations? 3
Number of in-scope critical systems (servers, routers, firewalls, etc. excluding desktops/laptops) (# of IPs) across all locations: 20?
Number of in-scope desktops/laptops across all locations: 100?

Are you interested in a wireless security assessment? (Y/N): Y
How many locations: 1 location, 2 SSIDs