CITY OF PASO ROBLES

IT STRATEGIC PLAN AND RISK ASSESSMENT QUESTIONS

January 31, 2018

Questions from GRC as a Service, LLC

- What regulatory compliance laws and mandates is the City operating under? Please list them.
  California General Law City

- Is the City required to be PCI DSS v3.2 compliant in any capacity as a Merchant or Service Provider? Please specify the Merchant Level/Tier if you know and what SAQ you submitted last year.
  Determining need is part of this project

- Is this security risk assessment needed to support a regulatory compliance, annual security risk assessment requirement (i.e., HIPAA, PCI, Privacy, other, etc.)? If yes – please specify.
  Determining need is part of this project

- What vendor/manufacturer and version of operating system software for Programmable Logical Controller's (PLCs) and SCADA equipment does the City have currently?
  Interviewing for this information is part of this project

- Other than the 7 Key Depts listed in the RFP, are there any other key Department Heads or executives that should be included in the interview list?
  We have 7 departments including the City Manager

- Does the City have its own legal/general counsel or is this outsourced by the City? Please state the name of the law firm if outsourced and if they will be available for interviews.
  The City has a contracted City Attorney

- Please provide an IT Org Chart and SCADA Org Chart indicating who is responsible for:

    - Workstations/Laptops (OS, Images, Standards, Anti-Virus, Anti-Malware, Applications, etc.)
    - LAN (Windows Active Directory/domain Controllers & LAN Switches Layer 2/Layer 3)
    - LAN to WAN (Internet Ingress/Egress, DMZ/VLAN, FW, IDS/IPS, Perimeter Security)
    - WAN (MPLS/WAN, Metro Ethernet, Other)
    - Remote Access (Citrix, IP_SEC/VPN, Multi-factor/Two-factor authentication, etc.)
    - Systems/Applications (Windows, Linux, VMware, Servers, OS', Applications, etc.)

  I.T. cross trains and shares the responsibilities of all these duties

- Please list your current hardware & software technology standards for both the IT side of the fence and the SCADA side of the fence:

    - Workstations/Laptops (Dell/HP/Acer, etc. / Windows XX, A-V, A-M, encrypted hard drives?)
    - LAN (Windows Active Directory/domain Controllers & Cisco LAN Switches Layer 2/Layer 3)
    - LAN to WAN (Internet Ingress/Egress, DMZ/VLAN?, FW Model?, IDS/IPS Model?, Perimeter Security?)
    - WAN (MPLS/WAN, Metro Ethernet, Pt to Pt VPN?)
    - Remote Access (Citrix, IP_SEC/VPN, Multi-factor/Two-factor authentication?)
    - Systems/Applications (Windows, Linux, VMware, Servers, OS', Applications?)

  Interviewing for this information is part of this project

- How many documented policies and procedures do you currently have in place for IT and IT security/privacy and for the SCADA environment and operations? Please list the names of your existing policies and procedures.
  Interviewing for this information is part of this project

- When was the last time you conducted a security risk assessment for the IT or SCADA environment?
  A formal assessment has not been completed for a long time

- Given the fixed budget mentioned in the RFP, does that mean the City at this time does not want to include security testing (Vulnerability assessment scanning, penetration testing) in the security risk assessment?
  The City is interested in consultant's opinion of what is needed for the assessment. If additional funds are required, they should be indicated.

    - If the City does desire security testing, please specify how many IP hosts are in scope for the following:

        - SCADA IT infrastructure environment (External – public facing IPs):
        - SCADA IT infrastructure environment (Internal):
        - City IT Infrastructure environment (External – public facing IPs):
        - City IT infrastructure environment (Internal):

- Which IT infrastructure is bigger: IT environment or the SCADA environment? Please specify the total # of active IP host devices and IT assets for each (minus printers and peripheral devices).

The IT infrastructure is larger with a little over 200 computers in 8 different facilities and multiple vehicles. Contractors do most of the SCADA support.

- What is the desired start date and end date of this project?
  The City is interested in starting the project as soon as reasonably possible

- With a 5-year strategic plan, does the City require a 5-year financial model to support the IT and IT security initiatives defined?
  Indicating how the costs of implementing the plan would lay out over 5 years is expected

- Will any modifications to the City's Professional Services Agreement be considered by the City?
  Reasonable requests will be considered

Questions from Seven Outsource

1. Whether companies from Outside USA can apply for this? (like,from India or Canada)

We do not feel a company without an onsite presence can do this project as well as needed

2. Whether we need to come over there for meetings?

Yes onsite meetings will be required

3. Can we perform the tasks (related to RFP) outside USA?

(like, from India or Canada)

We do not feel a company without an onsite presence can do this project as well as needed

4. Can we submit the proposals via email?

Yes