City of Doral
ITN No. 2024-05
Independent IT Audit
Addendum No. 2

Please note the following changes to the above-referenced solicitation (words underlined are additions):

Article 3 – SCOPE OF WORK / TECHNICAL SPECIFICATIONS
* * *
3.2 Qualifications & Experience

The City wishes to engage a firm that has significant experience and expertise in IT security, digital forensics, and penetration testing. The Awarded Proposer must have experience auditing IT infrastructure for public sector entities or within similarly complex and sensitive environments. The Awarded Proposer must also have the capacity to develop an IT audit work plan considering the City's budget constraints, priorities, and capacities. In the event the City engages the Awarded Proposer to conduct penetration testing of, or otherwise access, criminal justice information, such Awarded Proposer will be required to comply with all applicable FDLE Criminal Justice Information Services (CJIS) requirements.

The following questions were received. Answers are as indicated below.

1. Is government experience mandatory? Is similar experience with commercial clients acceptable?

   Answer: Government entity and similar public sector experience is not mandatory but is highly preferred.

2. Data Handling: What specific procedures will be followed to handle and protect data during the digital forensic analysis?

   Answer: Industry best practices will be used to handle and protect data. The proposer will ensure that it will not retain any city data after the engagement.

3. Analysis Tools: What digital forensic analysis tools and software does the City currently have, and are there any preferences for tools the proposer should use?

   Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

4. Access Control: Can you detail the current access control system and its configuration for the City's network file shares?

   Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

5. Change Management: How are changes to folder permissions currently tracked and managed within the City's IT infrastructure?

   Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

6. Audit Trails: What kind of audit trails are available for access and permission changes since 2018?

   Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

7. External Access: Are there any known instances of external access to the file shares, and how were they addressed?

   Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

8. Documentation Standards: What standards does the City require for the documentation of digital forensic analysis findings?

   Answer: Industry best practices for documenting findings during a security audit.

9. Security Framework Compliance: Which security frameworks (e.g., NIST, ISO) does the City adhere to, and how should the proposer ensure compliance during the audit?

   Answer: NIST. The proposer will ensure that the city complies with NIST guidelines and highlight areas that do not follow those guidelines.

10. Prioritization of Components: Within the scope of work, are there components that the City prioritizes over others?

    Answer: Yes. Critical areas will be discussed with the awarded proposer.

11. Access to Systems: Will the awarded proposer have unrestricted access to all necessary systems and data to perform the comprehensive audit?

    Answer: The awarded proposer will work with the system owner to perform the audit. Unrestricted access will not be provided as this poses a security risk.

12. Post-Audit Support: Is there an expectation for ongoing support or consultation after the initial report is delivered?

    Answer: Yes, the awarded proposer will work with the city to address any and all findings. Remediation recommendations will be provided after the engagement.

13. Incident Response: In the event that a breach is identified, what immediate actions does the City expect from the proposer?

    Answer: If a legitimate breach is identified, the awarded proposer will notify the city immediately and will disengage from the security audit until the incident response procedures are completed and the city is no longer affected.

14. Format of Deliverables: Can the City provide guidance on the preferred format and detail level for the audit outcomes and recommendations report? How many IT policies and procedures need to be reviewed?

    Answer: The awarded proposer will use industry best practices in formatting audit and recommendations reports.

15. How many systems do we need to review the access controls?

    Answer: Access control and Folder Shares

16. On average how many users are per system?

    Answer: All city employees.

17. Are access controls centralized or each system has its own access control mechanism?

    Answer: Centralized.

18. Do you have folder's audit logs since 2018?

    Answer: Some systems still have logs, others do not.

19. How big are the folder's audit logs in GB?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

20. Are the folders that need to be assessed still in use?

    Answer: Yes

21. Are the elected official file shares in a Windows environment? If not specify.

    Answer: Yes, Windows.

22. How big is the server/host that has the file shares?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

23. Is the server/host hosted on-premises or in the cloud? What type of file system is used for network shares (NFS, CIFS/SMB, etc.)?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

24. What mechanism has historically been utilized to control access to in-scope file shares (Active Directory, Novell, etc.)?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

25. The stated desire is to perform an access and administrative audit going back as far as 2018. Does the city have ALL access and administrative logs for the covered time period? If so, what types of logs exist (e.g. Windows Security Event Logs, syslog, etc.)?

    Answer: We have some application logs available.

26. How many servers are involved in the file system audit?

    Answer: One.

27. Section 3.3 includes the phrase "…will include, but not be limited to, the following components:" when referencing the scope of the engagement. How should bidders plan on pricing what appears to be an open-scope engagement? T&E?

    Answer: This solicitation is an Invitation to Negotiate, which will involve the scoring of proposals in accordance with the proposer's qualifications and other criteria as set forth in Section 2.4 of the ITN. Negotiations on exact scope and pricing will take place thereafter. Please refer to Section 2.3 for additional information concerning the evaluation process.

28. Section 3.3 states that (30) top-level folders are in scope. How many sub-folders, total objects, etc. are expected within the targeted environment?

    Answer: The exact number is not available at this time. Top-level folders each have about 5 to 10 folders, approximately.

29. Assuming that during the audit, log events will show access (proper or otherwise) by PAST employees and further assuming that the former employees' accounts have been removed, does the city have a mechanism to map the GUID within the log entry to a proper display name or is the expectation that the awardee provide this service?

    Answer: The city will provide a proper display name. The awardee must have the capability to do so in the event that the city cannot.

30. Does the city have any mechanism in place to identify protected data beyond directory location (e.g. data tagging, etc.)?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

31. Since the answers to the above and other questions may have a significant impact on responses, we would like to request that the ITN due date be extended by 30 days.

    Answer: The ITN has been extended as noted in Addendum No. 1.

32. Is government experience mandatory? We have similar experience with commercial clients, is that okay?

    Answer: Please refer to the response to question 1 above.

33. Can the qualified proposer provide the services remotely, specifically outside of the United States but with a regional presence (LATAM)?

    Answer: The awardee must be located within the United States.

34. Should it be 100% onsite?

    Answer: The scope of work may be done remotely if necessary, from within the United States. The City reserves the right to require performance on site at its sole discretion.

35. Can a subsidiary or subcontractor be used to perform the services described herein?

    Answer: The proposals submitted in connection with this ITN will be evaluated in substantial part based upon the qualifications of the proposer and its team. The services cannot be subcontracted.

36. Are permissions or policies for folders on shared files done locally on the servers, through the domain controller, or through a privileged access manager solution?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

37. In order to improve the city's security posture, should the offeror perform a security maturity assessment to validate the current security status of the entity?

    Answer: The final scope will be as required by the City within the parameters set forth in Section 3.3 of the ITN.

38. Is it mandatory to have key personnel within the geographic area where the audit service is going to be executed or can they be remotely?

    Answer: Please refer to the response to question 33 above.

39. Can we provide a list of similar audit, digital forensics and penetration testing projects within the last 5 years deployed but in other countries where the bidder provides cybersecurity services?

    Answer: Similar projects from outside the United States may be submitted for review. However, the selected proposer must be within the United States. The audit must be conducted from within the United States.

40. Can you provide the approximate volume or number of shared file folders and/or file servers that the City currently has?

    Answer: The requested information is sensitive in nature as it relates to the City’s current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

41. 1) ¿Can you tell us the location of the infrastructure (Datacenters, Clouds, On premises)? 2) ¿Could you provide us with more information about the organization? For example quantity of number of sites current or give us a normal pattern of “the City” in terms of employees, technological resources, etc. in order to quantify more accurate the costs of the services. 3) ¿Can you provide us with the number of assets (PCs and servers) that will be part of the audit, penetration testing and digital forensics (DFIR) service? 4) ¿Should we consider incident response (IR) services to complement digital forensics? If yes, specify whether the service can be offered through a pool of annual hours (60, 100, 120, etc.) 5) Provide a list with the number and types of network devices, IP phones, security platforms, services, applications, etc. that allows us to appropriately size the audit, pentesting and DFIR services.

    Answer: The requested information is sensitive in nature as it relates to the City’s current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

42. Can you indicate whether the penetration testing will be internal or external?

    Answer: Internal and external testing.

43. How many URLS, Domains or Subdomains will be evaluated at each site? ¿Can the pentesting be done in a white, black and gray box? Or is it left to the free choice of the offeror? Should we include retesting? ¿How many Ethical Hacking (EH) exercises should be performed per year? If you answer is affirmative, Indicate frequency: Monthly, Quarterly, Biannual?¿Can you deliver us with a list of internal and external web applications?¿Are there legacy applications published facing the Internet? How many? ¿Do you have any platform or security control that are masking or protecting their published websites? For example WAF, DDoS, CDN, ADC, etc. Should we remediate and/or mitigate the vulnerabilities and breaches found in the penetration test? Or will City of Doral security personnel do it?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

44. 1) Could you indicate if the pentest evaluation will be carried out only in IT or should we cover other areas? For example: • Industrial systems (SCADA) • Custom Web Applications. • Mobile iOS/Android Applications. • Wi-Fi, Internal and Perimeter Networks. • Social Engineering Campaigns. • Among others Also indicate the size of the area (Small, Medium, Large) 2) To provide the ethical hacking service, should probes or virtual machines (VMs) be placed in the network to scan or launch simulations of attacks on the assets. ¿Can The City provision the VMs with the minimum technical specifications provided by the supplier or VMs must be considered by the offeror? 3) ¿Who will implement the modifications or new policies in the security controls? ¿Provider or City of Doral security personnel? 4) Indicate if the service should include any training or awareness program for the security staff 5) Specify or define the period in which this service must be executed. For example: max. 3 months

    Answer: The City currently contemplates penetration testing evaluation will be carried out via Wi-Fi, Internal and perimeter networks. The City reserves the right to negotiate the final scope pursuant to the terms of the ITN.

45. Please list the location(s) of records and systems they are stored that could be used in providing the information requested in the RFP.

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

46. Please list the location(s) of records and systems they are stored that could be used in providing the information requested in the RFP.

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

47. For the Proposer's Experience section of the response, does City want vendors to include the required Proposer Qualification Statement or is City looking for something different here?

    Answer: The Proposers are required to submit a proposal package in accordance with the proposal submittal instructions set forth in Section 2.2 of the ITN. The information provided in the Proposer Qualification Statement, which is a part of Exhibit A of the ITN and should be part 6 of the proposal package, should be consistent with the remainder of the proposal.

48. What is the size/staffing and structure of the City's IT department in all areas relevant to the ITN?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

49. What is the size and structure of the City's current internal audit team?

    Answer: The requested information is sensitive in nature as it relates to the City's current security protocols and may pose a security risk if disclosed. As such, the information is exempt from public disclosure pursuant to Chapter 119, Florida Statutes. The City will work with the awarded proposer to provide and review this information once engaged.

50. Are the audit services fully funded or will any contract be contingent upon securing funding?

    Answer: The contract amount and funding sources are to be determined and will be upon completion of the negotiations between the City and awarded proposer.

51. Will the City consider extending the due date to 03 April?

    Answer: The deadline has been extended to the date set forth in Addendum No. 1.

52. Has City had this type of audit performed since the file structure was set up in 2018?

    Answer: Similar audits have been performed.

53. Are there documented folder access policies, procedures, standards, and guidelines in place? If so, how many?

    Answer: Yes. The City will work with the awarded proposer to provide and review this information once engaged.