DFW DALLAS
FORT WORTH
INTERNATIONAL
AIRPORT

November 17, 2020

CLARIFICATIONS NO.1

Re: Solicitation No. 7007011, Penetration Testing Services

Please be advised of the following clarifications to the above referenced Solicitation.

Q1. Under section 4.6.1, we do not see Internal Penetration Testing listed. Is it the intention of this RFP to have the contractors submit bids for just External Penetration Testing and Reporting? If Internal Penetration Testing should have been included under section 4.6.1, will DFW be providing additional information for the Internal Penetration Testing?

A1. The Internal and External scopes are the same except that the Internal Testing must be done onsite.

Q2. 4.6.1.1.1 states, Number of IP addresses in target space(s) – Approximately 3,500 while 2.2.1 states, Approximately 5,000 IPs. Is the target external space 3,500 IPs or 5,000 IPs?

A2. 5000 IP’s.

Q3. Is an objective of this testing to also assess the Company’s intrusion detection capabilities?

A3. Yes.

Q4. Are the external facing systems, referenced in section 2.2.1, 2.2.2, or 2.2.3, hosted by a third-party provider?

A4. This is a hybrid environment. We have third-party provider devices that third-party providers manage, however, the scope is to target DFW devices and not third-party devices.

Q5. Does your organization own and manage the network equipment at your external perimeter?

A5. Yes.

Q6. Can internal networks be scanned via a primary location or would it be necessary to perform field visits to more than one in-scope location?

A6. Field visits for all internal work.

Q7. Are any of the internal application a third-party provider?

A7. There should be less than 10.

Q8. For Physical Facility Breach, to what level should the unauthorized access be demonstrated? (access to paper files, office areas, network access, obtaining equipment, etc.)?

A8. The Vendor should work closely with the Project Lead for escorting and guidance.

Q9. Says not Exploit in 2.2.5, please confirm what all that applies to.

A9. Do not cause operational system outages. The Vendor should work closely with Project Lead.

Q10. 2.2.4 states, Scan DFW's Guest Wi-Fi network for any rogue device traffic. How many locations are in scope for this Guest W-Fi scanning?

A10. In 7 locations. (Airport Headquarters, 5 Terminals and Rental car center)

Q11. How many SSIDs and which locations?

A11. Perform a discovery scan and identify the SSID's in the entire DFW network.

Q12. 4.6.1.1.6 states, Number of Wireless Networks – 6 connections. How many SSIDs and which locations?

A12. Perform a discovery scan and identify the SSID's in the entire DFW network.

Q13. Under 4.6 in the requirements section, it states that testing should meet ISO 270001 and PCI-DSS audit requirements. Can you provide approximate number of systems (IP addresses) that fall into your PCI scope and those that fall under your ISO 270001 criteria?

A13. Approximately 35, and they all fall under ISO 270001 criteria.

Q14. Is it acceptable to structure the final report to comply with NIST 800-53 controls which encompasses both ISO 270001 and PCI-DSS controls criteria?

A14. Yes.

Q15. Are only technical controls associated with ISO 270001 and PCI-DSS controls in scope or are policy and procedural controls also include?

A15. Technical controls are in scope, however, we are open to considering recommendations from the awarded Vendor.

Q16. Are existing policies and procedural (workflow) controls consolidated into a single or small number of documents?

A16. A small number of documents.

Q17. Is OWASP standard application testing appropriate for target web applications or is credentialed based assessment required?

A17. Standard application testing.

Q18. Is there an estimate of total "active" IP addresses for the external and internal components of this RFP?

A18. 5000 IP's.

Q19. Based on the request timeline and IP Scope (15,000+) is sampling of certain network ranges acceptable or are all active IP addresses in scope and required to be assessed?

A19. All active IP addresses in scope are to be assessed.

Q20. Can assessment activities be performed both during work hours as well as after hours?

A20. During standard work hours (8:30 a.m. to 5:00 p.m. Central Time Monday through Friday). If after hours work is needed the Vendor should seek approval form the Project Lead.

Q21. Are/which target network ranges are accessible from a centralized location(s)?

A21. This is a Black box testing and we leave this to the Vendor to decide.

Q22. Will a single chaperone/resource be provided that can provide SHI access to all the physical testing locations or will we need to coordinate with multiple resources?

A22. We (DFW employees) will escort the resource to all the physical testing locations.

Q23. Can multiple technical assessments be launched simultaneously?

A23. Yes, but the Vendor will need to coordinate with the Project Lead.

Q24. Will DFW Airport consider responses with a timeline longer than 4 weeks?

A24. No, this project must be complete by the end of the year.

Q25. If yes to the above, what is the longest timeline for completion of the assessment the Airport will consider? How much flexibility does the Airport have for completing this project?

A25. The work must be complete by the end of the year.

Q26. Given the short window between when vendor questions are due and the final bid due date, in order to provide ample time for all vendors to submit complete and accurate responses, will DFW Airport extend the bid due to date to two weeks after the Airport issues answers to all vendor questions that have been received?

A26. No, DFW is up against an end of the year deadline for this project.

Q27. If no to the above, will DFW Airport extend the bid due by at least one week (not including Thanksgiving Day - to 12/1)?

A27. See Answer 26.

Q28. Will vendors only need to complete the 1295 form upon award, or upon proposal submission?

A28. The 1295 form must be completed upon request, after award.

Q29. What is the reasoning for procuring this contract for a period of 6 months?

A29. Six-month timeline is to allow for invoicing, payment and any unforeseen problems.

Q30. What is budgeted for this six-month contract?

A30. The budget will be determined at the time of award.

Q31. Will DFW request individuals performing the work to sign a Non-disclosure Agreement (NDA) under this contract, or will the contractor (company) NDA cover all individuals (employees) under this contract as normal?

A31. A non-disclosure agreement is not required.

Q32. If this will be requested can DFW please provide a copy of the NDA in advance?

A32. See answer 31.

Q33. Page 30 of the RFP mentions SOC II and ISO and FedRAMP under 5.11 Audits and Assessment Reports. What are vendors expected to report regarding these certifications, if anything? a. Are vendors expected to hold these certifications, and if so, what is the reasoning and how does it relate to the scope of this contract?

A33 Upon request from Audit these items are expected to be produced.

Q34. Qualifications page 22 asks that contractors shall provide resumes for those performing work with proof of… then lists certifications. Are vendors required to include copies of the? certifications in their proposal or can vendors notate which certifications each team member has in their resume.

A34. No need to attach certifications. Just resumes showing the vendor members are certified and eligible as mentioned in the scope of the work.

Q35. Although each Phase lists the timeframe in number of weeks in the RFP, can vendors propose an alternative time frame?

A35. If they can finish the project in the given 4 weeks within the calendar year of 2020 an alternate plan may be considered.

Q36. The RFP shows that there is a physical aspect to entering the facilities, does DFW anticipate any use of social engineering techniques to gain entry?

A36. There are security guards monitoring. The scope of work for the Vendor is to find vulnerabilities to gain entry by using social engineering techniques or any alternate ways.

Q37. Will phishing be part of this engagement?

A37. Yes.

Q38. Section 2 Phase 1 of the RFP outlines External Penetration Testing requirements, then section 4.6.1.1 outlines External Penetration Testing again. Which External Penetration Testing requirements should vendors follow. If both, what is the reasoning for outlining this twice?

A38. There should be one External and one Internal only.

Q39. Will vendors only need to complete the 1295 form upon award, or upon proposal submission?

A39. Upon request upon award.

Q40. What is the reasoning for procuring this contract for a period of 6 months?

A40. Six months will allow for all invoicing, payments and any unplanned for events to be resolved.

Q41. What is budgeted for this six-month contract?

A41. Budgets will be set at the time of award.

Q42. Will DFW request individuals performing the work to sign a Non-disclosure Agreement (NDA) under this contract, or will the contractor (company) NDA cover all individuals (employees) under this contract as normal? If this will be requested can DFW please provide a copy of the NDA in advance?

A42. Non-Disclosure Agreements are not required for this project.

Q43. Page 30 of the RFP mentions SOC II and ISO and FedRAMP under 5.11 Audits and Assessment Reports. What are vendors expected to report regarding these certifications, if anything? Are vendors expected to hold these certifications, and if so, what is the reasoning and how does it relate to the scope of this contract?

A43. Yes. This is a security requirement from DFW.

Q44. Do we need to perform External Penetration Testing on all the components that are owned by DFW (such as 5,000 IPs and Domains including the DFW's external facing website, excluding IPs assigned to Non-DFW devices)? Please clarify.

A44. No, not to non-DFW devices. Only DFW external-facing websites.

Q45. Do we need to perform External Penetration Testing on all the DFW's network connected devices which are associated with 10,000 IPs?

A45. The Vendor should do a discovery, identify all the IP's that are in DFW network, and perform a penetration test.

Q46. Do we need to perform Internal Penetration Testing on all 4,500 DFW's internal servers and workstations devices?

A46 Yes. The Vendor should do a discovery, identify the OT assets and perform the penetration test.

Q47. Do we need to perform Internal Penetration Testing on all the 10,000 IP-based OT assets (IoT, ICS, SCADA)?

A47. Yes. The Vendor should do a discovery, identify the OT assets and perform the penetration test.

Q48. Please share below details for Internal Network Vulnerability Assessment and Penetration Testing?

- **Number of IP addresses in target space(s)**
- **Number of Internal live hosts (Websites), approximately**
- **Internal Website(s) for Vulnerability Assessment and Penetration Testing**
- **Number of Wireless Networks**
- **Number of Local audio intercom system/Public Address System (PAS)**
- **Number of Fire and Smoke Alarm devices**
- **Number of heating, ventilation, and air conditioning (HVAC) system**
- **Number of Wire plant network systems**
- **Number of Lighting Systems**
- **Number of IoT, ICS, SCADA devices**
- **Number of Internal network (wired and wireless)**

A48. The Vendor should do a discovery, identify the OT assets and perform the penetration test. Approximately there would be about 10,000 Ip's all together.

Q49. what type of social engineering techniques do we need to perform in (12) External Building(s)?

A49. Piggybacking and interviewing people (social engineering questions).

Q50. Will you provide Wi-Fi access to Vendors in (12) External Building(s)?

A50. Vendors can use Guest Wi-Fi.

Q51. When does DFW anticipate issuing responses to vendor questions?

A51. As soon as they are available.

Q52. Please clarify if DFW is requesting for the vendor to exploit/attempt penetration or not. The requirement seems contradictory and contradicts sections 4.6.1.1.1 and 4.6.1.1.4.

A52.Vendors should scan and find the vulnerabilities and provide the screenshots or evidence with potential possible for a breach. Do not break in or exploit.

Q53.What form of proof should the vendor provide?

A53. No certification proof is required to submit. We want certified pen testers to perform the assessment.

Q54. Will you be providing generalized environment information such as # of servers, locations, employees? (Note, providing this information will significantly reduce the time/cost of the overall engagement).

A54. This is a Black box pen test. Do a discovery and identify the assets. Locations are provided in the SOW.

Q55. Are there specific Company names associated with the business other than the current operating name? If so, what are they? Are they in scope of the exercise? Will they have any limitations, specific to that company, that are different than the overall scope?

A55. No.

Q56. Will we be profiling all employees or just a specific sample set?

A56. This is not in the scope.

Q57. Will we be profiling all executives or just a sample set?

A57. This is not in the scope.

Q58. Will we be profiling 3rd parties or associates of the company?

A58. This is not in the scope.

Q59. At what depth would you like to profile the selected subjects (ex: social network analysis, behavior analysis, personality profiling, potential harm profiling, ability to capture corporate asset, ability to extract human asset or intelligence asset…etc.).

A59. This is not in the scope.

Q60. Would you like to test the ability to extract intelligence for collected or identified human assets?

A60. This is not in the scope.

Q61. How many separate facilities/buildings exist on the DFW airport site?

A61. 13 locations.

Q62. Would you like to identify the ability to gain access to public record, blueprints and other facility diagrams?

A62. This is not in the scope of work.

Q63. How many physical locations would you like assessed?

A63. 13.

Q64. What is the square footage of each location?

A64. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q65. How many floors are in each location?

A65. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q66. How many employees work at each location?

A66. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q67. Are the facilities secured by onsite guards? Are they onsite 24x7? Are the guards armed?

A67. Yes.

Q68. How many locations are to receive physical assessment?

A68. AHQ and all 5 Terminals.

Q69. Would you like physical penetration testing to be performed or an authorized survey?

A69. Piggybacking and social engineering by interviewing employees.

Q70. Would you like to test converged attack surfaces?

A70. No, this is not in scope.

Q71. What type of access controls are used (RFID, HID, RF, Standard key, etc.)? Would you like us to identify/exploit vulnerabilities within the physical access control systems? Are alarm systems used? If so, what type? Would you like us to identify/exploit vulnerabilities within the alarm systems to show the ability to access or bypass? Is physical alteration in scope (breaking glass, limited damage to low value replaceable goods, destruction of keyways, cutting of padlocks etc.).

A71. No, this is not in scope.

Q72. How many locations are to receive wireless assessment?

A72. Airport Headquarters, All 5 Terminals, Rental Car Center, Department of Public Safety Center.

Q73. How many wireless access points are at each location?

A73. A Vendor must scan to discover.

Q74. Would you like a site survey mapping AP location?

A74. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q75. Would you like active attacks to attempt to gain unauthorized access to wireless networks?

A75. Yes.

Q76. How many wireless networks would you like assessed?

A76. The Vendor must discover and assess.

Q77. What types of sensitive data do you store? (Credit Cards, Medical Records, Financial Data, Employee Records)

A77. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q78. How many different applications store Sensitive Information?

A78. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q79. How many application administrators support these applications? For each, are the data flows, access methods, and asset locations documented? How many individual PII/CC and other Compliance regulated data storing applications are there? How many of these applications are developed internally? How many development teams support these applications? How many of these are web-based?

A79. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q80. How many different Business Units are there within the organization?

A80. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q81. How many separate IT groups support the infrastructure?

A81. Due to the sensitive nature of Penetration Testing, we are unable to provide this information in this solicitation; however, the contract awardee will be provided this information to perform the work.

Q82. How many IT staff members are within each group? Could you please list the type of information or asset you feel are the "most critical" to protect?

A82. All DFW operational assets are mission critical.

Q83. Would you like to identify if we are able to access this information asset? Would you like to validate if extraction of the asset is possible? Will external phishing be required for this assessment?

A83. Yes.

Q84. Approximate number of users targeted?

A84. 100.

Q85. Will phone conversations/pretexted be required?

A85. Yes.

Q86. Approximate number of users targeted?

A86. 25.

Q87. Are you interested in onsite social engineering (tailgating, impersonation, media drops, etc.)?

A87. Yes.

Q88. How many attack scenarios or attack iterations would you like to test?

A88. 5.

Q89. Will environmental access persistence be a requirement of testing? For what length of time will persistence exercises need to be tested? What access persistence types will need to be demonstrated (physical, electronic, social)?

A89. This is not in the scope.

Q90. Will long-term asset/IP access be required to demonstrate? For what length of time?

A90. This is not in the scope.

Q91. Will long-term/constant exposure be in scope? (Altering batch jobs, scripted tasks, automated functions to show stainable long-term loss or access)?

A91. No. This is not in the scope.

Q92. Will Blue Team or Defensive Assessment be required as part of this engagement?

A92. No. This is not in the scope.

Q93. Is there a dedicated Incident Response (IR) Team?

A93. Yes.

Q94. Will we be a known or unknown element to the team?

A94. Unknown.

Q95. Would the engineer be requested to augment and help lead the IR team or purely observe the effectiveness of the team?

A95. Purely observe.

Q96. Are there well-defined IR processes?

A96. Yes.

Q97. Will we be looking to track and identify gaps in current IR process?

A97. No.

Q98. Will active analysis of IR techniques need to be assessed?

A98. This is not in the scope.

Q99. Will the IR team be within the scope of the assets/individuals slated for exposure testing?

A99. No.

Q100. Will the adversarial engineers be able to interact directly with the IR team during the attack to identify the likelihood of direct compromise?

A100. Work with Project Lead only.

Q101. At what length of time would you expect to engage in Blue Team assistance/assessment? (ex. The entire engagement, just during specific attack types, start and finish of project, or other)

A101. The entire engagement.

Q102. For 3.1.1.10 USB port scanning what is the estimated count of ports to test?

A102 The Vendor should randomly select a few random ports in all 5 Terminals.

Q103. For 3.1.1.12 Ethernet port in terminals what is the estimated count # of jacks of testing each enabled/disabled?

A103. The Vendor should randomly select a few random ports in all 5 Terminals.

Q104. For 4.6 in relation to PCI/DSS will this need to be covered in scoping of what segmentation of the network is identified specifically to PCI DSS? Will this data be used for self-attestation only or are their requirements for ASV or a QSA for the selected vendor?

A104. ASV for a specified vendor.

Q105. Please identify the projected timeline expectation of completion of this testing from kickoff call to reporting.

A105. 4 weeks.

Q106. Please identify if this type of testing is executed annually or more frequency. When was the last testing completed?

A106. Annually. The last test was completed in 2019.

Q107. Will there be any information shared to the chosen vendor on specific findings from previous tests to validate remediation or known weaknesses or areas of concern?

A107. The previous results are confidential.

Q108. For the internal testing/Physical security components are there any blackout dates or periods where testing could not be performed.

A108. No.

Q109. Does DFW have a preferred timeframe mm/dd to begin the testing?

A109. 12/03/2020. Approximately.

Q110. On the Scope of Work Section (SOW), we see that the project is broken into three (3) phases over the course of four (4) weeks. Can these 3 phases be spread across a longer duration than four (4) weeks to complete the SOW?

A110. Based on the previous Pen test projects, we have assigned week 2 and week 3 for internal testing. All we need is to complete the project in 4 weeks and the vendor can work with project lead regarding timings and flexibility.

Q111. Can a portion of the internal scoped items have reconnaissance performed remotely prior to onsite execution?

A111. Internal tests should be done onsite.

Q112. Does DFW have a no later than date in mind for the completion of this Network Vulnerability Assessment and Penetration Testing?

A112. The completion date is by end of Dec 2020.

Q113. Has DFW experienced a penetration test prior to this RFB?

A113. The last Pen test was performed in 2019.

Q114. Page iv, Solicitation Summary, Item 1. General Description. The paragraph ends with "The scope of external and internal penetration testing shall include:" – is it safe to assume that the expanded information is the same as what is provided starting on page 10 under Specifications/Scope of Work?

A114. Yes, the Specifications/Scope of Work is the expanded information.

Q115.Please confirm that we are to submit only one copy of our proposal.

A115. Confirmed.

Q116. Due to COVID will you please consider accepting responses via email?

A116. Email responses are not acceptable.

NOTE: A copy of this questions and clarifications shall be acknowledged by appropriate signature and attached to the submitted proposal.

____
Company Name

____
Signed Date

If you have any questions regarding this matter, contact during normal working hours (8:00 AM to 4:30 PM, Monday through Friday) email address of pwatkins@dfwairport.com

Sincerely,
Peggy J. Watkins
Contract Administrator
Procurement and Materials Management Department