METROPOLITAN WASHINGTON
AIRPORTS AUTHORITY

RFP No. 1-15-C017
OFFICE OF TECHNOLOGY INFORMATION SYSTEMS AND INFRASTRUCTURE PENETRATION TEST

Questions and Answers

Notice: Questions may have been edited for clarity and relevance.

1. How many desktops, laptops, and other peripheral systems are on the internal network?

   ANSWER: There are approximately 4,000 nodes on the internal network.

2. What different operating systems are in use for desktops and laptops?

   ANSWER: Not relevant.

3. Please describe the number of business applications that are considered Commercial off the Shelf (COTS), including their operating systems.

   ANSWER: Not relevant.

4. Please describe the number of business applications that are considered internally developed/maintained/programmed.

   ANSWER: Not relevant.

5. What third-party service providers are currently being utilized from an IT perspective: Infrastructure only providers? Data storage/processing/management providers

   ANSWER: Not relevant.

6. The locations are noted to be Dulles Airport, Reagan Airport and the Dulles Toll Road. Are these locations connected in any way?

   ANSWER: The sites are connected, although all networks in scope (i.e. independent network) may not be.

7. If one exists, what type of connection between location and available bandwidth?

   ANSWER: For the sites that are connected the bandwidth is more than adequate for a penetration test.

8. How many mobile devices with network access?

   ANSWER: Not relevant.

9. Is there a Bring Your Own Device policy in place?

   ANSWER: Not relevant.

10. How many WAPs are in use?

    ANSWER: There are approximately 90 in use.

11. How many locations will need to be tested for the wireless penetration test?

    ANSWER: All locations need to be tested.

12. How many data centers are to be tested?

    ANSWER: Not relevant.

13. Does MWAA provide any Infrastructure as a Service (IAAS) or Architecture as a Service (AaaS) to any other airport authorities?

    ANSWER: No.

14. Is social engineering considered in scope? This would include email phishing, pre-text calls, onsite social engineering.

    ANSWER: No.

15. Is the email system hosted internally or by a third party vendor?

    ANSWER: This information will be provided to the successful offeror after contract award.

16. Can you provide the number of full time employees and job titles for the following: Organization, current internal audit/IT audit/Risk, current internal IT department staff?

    ANSWER: Not relevant.

17. How many and what type of firewalls are in place?

    ANSWER: This information will be provided to the successful offeror after contract award.

18. Is administration of systems centralized or decentralized?

    ANSWER: Not relevant.

19. How many external/internet facing IP addresses are in scope for external testing?

    ANSWER: See SOW 4.2.1.

20. How many websites are running from the MWAA infrastructure?

    ANSWER: See SOW 4.2.4.

21. Please list the number of different number of operating systems in use.

ANSWER: Not relevant.

22. Please describe the internet facing systems/applications run by MWAA that are hosted on in-house systems.

ANSWER: This information will be provided to the successful offeror after contract award.

23. Please list any internet facing systems that are conducting some form of e-commerce.

ANSWER: This information will be provided to the successful offeror after contract award.

24. Please describe each form of remote access provided to staff, IT and/or vendors.

ANSWER: Not relevant.

25. Are there any hosted applications (not on your infrastructure) that should be considered in scope?

ANSWER: No.

26. Should any applications that are identified outside of the 10 indicated within the proposal be tested as well, with proper notification to MWAA?

ANSWER: No, they should be recorded, not tested

27. Please list the number of active directory domains in operation.

ANSWER: Not relevant.

28. Please describe any (centralized) authentication mechanisms in place.

ANSWER: Not relevant.

29. Please describe the number of in-house servers, including their operating systems. This information will be provided once the contract has been awarded.

ANSWER: See answer to question 1.

30. How many servers are virtualized?

ANSWER: This information will be provided to the successful offeror after contract award.

31. What is the virtualization technology in use?

ANSWER: This information will be provided to the successful offeror after contract award.

32. What comprises an independent network?

ANSWER: An independent network is a physical network not connected in any way to the primary or other networks.

33. Approximately how many independent networks are there?

ANSWER: There are approximately 11 independent networks.

34. Can you estimate how many IP addresses or subnets each of the networks may have?

ANSWER: Approximately 4,000 nodes for the primary network and up to 3,000 nodes for the independent networks.

35. Are any of the independent network industrial control or SCADA systems?

ANSWER: Yes.

36. Can you provide the number of full time employees and job titles for the following: Organization, current internal audit/IT audit/Risk, current internal IT department staff?

ANSWER: Not relevant.

37. As this is 0% LDBE participation requirement, would this procurement be considered "Full & Open," with firms of any size able to bid?

ANSWER: Yes.

38. Will MWAA provide login credentials for performing the web application testing in order to assess RBAC controls and more thoroughly test the 10 applications or is MWAA's intent to have the contractor perform unauthenticated web application testing?

ANSWER: No this is a non-credentialed unauthenticated exercise.

39. Please confirm that the external and internal testing will be performed from the perspective of outsider and insider without knowledge (i.e. no authenticated scans or credentials)?

ANSWER: Confirmed. See answer to question 38.

40. Under the SOW, for Web Application Penetration Testing, do you wish for the assessment of each site to be performed with or without credentials (or both)?

ANSWER: See answer to question 38.

41. Can reasonable travel costs for consultants outside the NCR be expensed back to MWAA as a separate line item?

ANSWER: The Authority contemplates award of a firm fixed-price contract resulting from this solicitation. Price proposals shall include all travel and related costs associated with performing the services required by the Statement of Work.

42. The scope of the SOW states '...several independent internal networks.' Approximately how many networks does this encompass?

ANSWER: See answer to question 33.

a. Are these networks air-gapped?

ANSWER: This information will be provided to the successful offeror after contract award.

b. Are the systems on these networks included in the approximately 4000 Internal IP addresses?

ANSWER: No. See answer to question 34.

43. Typically, external penetration tests, and most web application assessments, can be conducted remotely. Do you anticipate needing those assessments conducted on site?

ANSWER: No, any external (Internet facing) testing can be performed remotely.

44. Within the MWAAs web apps, how many pages per site?

ANSWER: Not relevant.

45. How many wireless networks does MWAA have, and how many at each site?

ANSWER: There are two wireless networks. Testing for rogue wireless networks shall be conducted at all locations.

46. What risk assessment framework-guidelines does the MWAA currently adhere to?

ANSWER: Not relevant.

47. Is MWAA looking for Best Value or Lowest Cost?

ANSWER: This is a best value solicitation.

48. Is Rapid7 eligible to bid for this opportunity, or will we need to work through an eligible reseller?

ANSWER: All qualified contractors may propose on this solicitation.

49. Here are some questions that will allow us to make sure we properly scope this engagement:

Internal Network Penetration Testing and Total number of active IPs (internal):

ANSWER: See answer to question 34.

Servers:

a. Total Server Count:

ANSWER: Not relevant.

b. Breakdown of Windows:

ANSWER: Not relevant.

c. Breakdown of Linux:

ANSWER: Not relevant.

d. Breakdown of Other:

ANSWER: Not relevant.

e. Workstations:

ANSWER: Not relevant.

f. Total workstation count:

ANSWER: Not relevant.

50. How many standard builds or images are you using to deploy these workstations (this is to see how much we will be able to take advantage of sampling)?

ANSWER: Not relevant.

51. Number of network devices (est.):

ANSWER: See response to question #1.

52. Application Penetration Testing

For the application penetration testing, the most important information for scoping purposes is to get an estimate of size of the application. This includes number of pages, number of user level roles (ie. Admin, User, etc.), whether the pages are mostly comprised of static or dynamic content, and how many unique input fields are being used across all pages. This information will provide a good understanding of how long and complex the testing of the application will be. With that in mind, please address the following questions to the best of your ability.

Application Penetration Testing Questions

a. How many applications are in scope for this security assessment?

ANSWER: See response to question #19

b. Is the application internal, or public facing?

ANSWER: External.

c. If public facing, please provide a URL for each app in scope:

ANSWER: Not relevant.

d. App1:

ANSWER: Not relevant.

e. App2:

ANSWER: Not relevant.

f. App3:

ANSWER: Not relevant.

g. Application No. 1:

ANSWER: Not relevant.

Sizing:

h. How many web pages comprise the application?

ANSWER: Not relevant.

i. How many of those web pages are static?

ANSWER: Not relevant.

j. How many of those web pages are dynamic?

ANSWER: Not relevant.

k. How many total input parameters are used (input fields across all pages)?

ANSWER: Not relevant.

l. How many unique input parameters are used (input parameters reused on several pages)?

ANSWER: Not relevant.

m. How many user levels or roles are defined within the application (ie Admin, User, Customer)?

ANSWER: Not relevant.

n. How many user roles are in scope for the testing?

ANSWER: Not relevant.

53. Wireless Assessment

a. Number of wireless networks in scope:

ANSWER: See response to question # 44

b. Number of wireless access points:

ANSWER: Not relevant.

c. Number of controllers:

ANSWER: Not relevant.

d. Number of locations (unique cities or geographical locations.):

ANSWER: There are three (3) locations.

i. For each building:

ANSWER: Not relevant.

ii. Number of floors:

ANSWER: Not relevant.

iii. Approximate square footage:

ANSWER: Not relevant.

54. Additional Helpful Questions

The following questions give additional depth to understanding your business, which allows context for our findings. Answers are not necessary at this point in time (as they will be asked during the assessment) but they are somewhat helpful in scoping the engagement (assist in understanding maturity level of security program within the organization).

ANSWER: Not relevant.

a. Additional questions that allows for more business applicable recommendations:

ANSWER: Not relevant.

b. Do you have a documented security program?

ANSWER: Not relevant.

c. Documented process and procedures?

ANSWER: Not relevant.

d. Incident response plan?

ANSWER: Not relevant.

e. How large is the organization?

ANSWER: Not relevant.

f. What is the structure of the organization (centralized or decentralized)?

ANSWER: Not relevant.

g. How many networks does the company maintain?

ANSWER: One (1) primary network and approximately 11 independent networks. See response to question #33.

55. During the assessment we will need:

a. Network Diagram

ANSWER: Not Relevant.

b. Documentation on Policies, Procedures, Methodology (as they relate to Security Practices)

ANSWER: Not Relevant.

c. Org Chart (IT Security team)

ANSWER: Not Relevant.

56. With respect to the Web Application Pen test, please indicate how many dynamic elements each site contains. Dynamic elements are either dynamically generated pages, Flash/Activex components and pages taking user input, possibly displaying derived data as a response, changing the information on a database or changing the application's state.

ANSWER: Not Relevant.

57. Regarding the Wireless Pen test, please clarify the amount (how many sites) and size (how many access points on each site, how many different networks connected to the access points, how many different levels of access provided by the APs) of the networks to be tested.

ANSWER: There are two authorized networks. Sites to be tested are Reagan National, Dulles International and Dulles Toll Road.

58. The statement of work mentions "... several independent networks...". These networks are not referenced again in any of the objectives. Will these networks be tested? If so, how many will be tested under each of the engagements indicated as task objectives in section 4.2? Are these networks already included in the IP address count for each task objective?

ANSWER: There are approximately 11 independent networks and all will be tested.

59. Do these 10 web applications have support for payment, file upload or other unusual characteristics? Do they support multiple users or user roles? If yes, how many roles or how are user privileges handled?

ANSWER: Not Relevant.

60. What is the composition of the internal network for the internal penetration test? What is the approximate number of workstations, servers and network devices and how is the network segmented (e.g. all hosts in one network, multiple networks of the same size, different networks of various sizes, etc)?

ANSWER: See answer to question #34. Segmentation is not relevant.

61. The Estimated Dollar Value states Up to $80,000. Is this the anticipated amount for all three years combined or for each year?

ANSWER: See Amendment 2.

62. When was the last penetration test performed and who was the vendor?

ANSWER: Not Relevant.

63. The Pricing Schedule states: Price evaluation will be based on the total price of the base period plus the two option years. Does this mean that whatever price we arrived at during the first engagement (year), the overall price will be multiplied by three for the base and two option years?

ANSWER: See Amendment 2.

64. Should the Price proposed by each vendor be for the entire duration of the contract (3 years)?

ANSWER: See Amendment 2.

65. How many times in each year does MWAA anticipate performing the penetration testing?

ANSWER: See Amendment 2.

66. For the Wireless Penetration Testing, how many wireless networks or Access Points (APs) are in the environment and how many are in each of the Places of Performance?

ANSWER: There are two (2) authorized networks.

67. For the Web Application Penetration Testing, you indicated 10 sites. Web apps testing could be very time consuming. Approximately how many pages are in each site? Are these sites password protected? If so, how many? Of these 10 sites, how many of them are internal and external?

ANSWER: The 10 sites are external with password protection but the number of pages is unknown.

68. Your work hours state: 9:00 am to 3:30 pm eastern time. Does the Authority expect the internal pen testing to be restricted to this time window?

ANSWER: Yes, it is expected that internal pen testing will occur within this schedule. The COTR and the contractor must mutually agree upon all deviations to this schedule.

69. What is the required citizenship status of proposed staff?

ANSWER: The Contractor shall ensure that it is in compliance with the Immigration Reform and Control Act of 1986.

70. When is contract award and work commencement anticipated?

ANSWER: Contract Award is anticipated early March 2015.

71. Reference Section VII, page 1, Paragraph 01: it states that the Contractor shall furnish all necessary labor, material, etc. to conduct Pen Test to identify and remedy security vulnerabilities. Can the Authority clarify if they are expecting remediation to be included as part of this proposal? If so, will the Contractor be allowed to adjust schedule and price after vulnerabilities have been identified?

ANSWER: Remediation is not within scope of this solicitation. See Amendment 2.

72. Reference Section VII, Page 2, Paragraph 9: it states that the Authority will not furnish any facilities. Can the Authority confirm that office space will be provided for worked that will be conducted at the Authority's locations?

ANSWER: The Authority will provide space for activities conducted at its locations.

73. Reference Attachment 01, Page 1, Paragraph 1: it states the purpose of the opportunity is to identify AND remedy security vulnerabilities. Can the Authority clarify how they wish the bidders to price remediation without performing the penetration testing activities which identify the number and severity of vulnerabilities that will need to be remediated?

ANSWER: See response to question 71 and Amendment 2.

74. Reference Attachment 01, Page 1, Paragraph 2: it states that the penetration test will be performed on the main network and several independent internal networks. Approximately how many independent internal networks does the Airport Authority desire the winning bidder to conduct penetration testing?

ANSWER: See answer 58.

75. Reference Attachment 01, Page 2, Paragraph 4.2.3: how many wireless networks does the Authority wish to have penetration testing performed? Is there one or multiple wireless networks per physical site Dulles, Reagan and Toll Road facilities?

ANSWER: There are two authorized networks for all facilities.

76. Reference Attachment 01, Page 2, Paragraph 4.2.4: what is the total number of web applications the Authority wishes to have tested?

ANSWER: Approximately 10.

77. Reference Attachment 01, Page 2, Paragraph 4.2.4: does the authority wish to have authenticated or un-authenticated application testing performed?

ANSWER: See answer to question 38.

78. Will past penetration testing results and security assessment results be provided to the winning bidder to validate previously identified vulnerabilities have been fixed?

ANSWER: No. Past results are not relevant.

79. Reference Attachment 01, Page 5, Paragraph 11: it states that work products shall be submitted IAW a later scheduled date determined by Authority. Can the Authority clarify how this date is different from the Contractor provided schedule? Also, will the Contractor be allowed to provide input on this date?

ANSWER: The Authority will coordinate final dates with the successful offeror.

80. Reference Attachment 01, Page 5, Paragraph 12: does the Authority require the Project Manager to have a CEH, CISSP AND GWAPT certification or just one of the three certifications listed?

ANSWER: One of the three

81. Reference Attachment 01 Page 2 Section 4.2.1 Is social engineering to be included in the scope of the external testing? This would include Email phishing or spear phishing to gain user credentials or phone based methods as well.

ANSWER: No. See response to question 14.

82. Reference Attachment 01 Page 2 Section 4.2.2 Is social engineering to be included in the scope of the internal testing? This would include media drops and physical security access.

ANSWER: No. See response to question 14.

83. Reference Attachment 01 Section 4.2 Since testing is non-destructive in nature will we be able to test during regular business hours or will testing be required to be scheduled after normal working hours?

ANSWER: See response to question 68.

84. Reference Attachment 01 Section 4.2.4 Should the Web Application security testing or should the scope be limited to network and system level exploits? Should Web application testing be limited to static testing or would dynamic testing be required?

ANSWER: All levels of exploits should be considered.

85. The Web Application Penetration testing states that: Contractor will conduct test of web applications approximately 10 sites. Can you confirm the exact number of web applications for testing?

ANSWER: No.

86. For each web application, can you provide the following information:

a. A short description of the business functionality.

ANSWER: Not relevant.

b. Does the application handle sensitive information e.g. PII, PCI, HIPAA, etc.?

ANSWER: Not relevant.

c. Approximately how many pages of the web application accept user input?

ANSWER: Not relevant.

d. How many user roles does the application utilize e.g. admin, customer, internal user.

ANSWER: Not relevant.

87. Indicate how the distribution of apps falls within the categories below:

Simple No authentication, limited to 10 dynamic pages or less
Medium User Authentication, up to 30 dynamic pages, and 2 roles e.g. user, admin
Complex User Authentication over 30 dynamic pages and/or more than 2 roles.
Or
Applications that include web services, mobile applications e.g. iOS, Android

ANSWER: Not relevant.

88. Will any testing be done on production web applications or will the web app security assessments be done within a test environment?

ANSWER: Production web applications.

89. Will web application pen testing be conducted from authenticated perspective? If so, how many roles are included in scope for each of the 10 sites?

ANSWER: See response to question 38. The roles are not relevant.

90. For the internal network testing portion, is the 4,000 IP address an estimate of active hosts on the network, or an approximation of the total IP address space? If approximation of total IP space, would it be possible to obtain an estimate of total hosts/nodes on the network?

ANSWER: See response to question 34.

91. How many physical locations will the assessor need to plug into in order to assess all network ranges? Can all internal networks be assessed from a single physical location e.g. DCA, IAD or Dulles Toll Rd Offices?

ANSWER: Three (3) DCA, IAD and DTR respectively.

92. Will any critical systems e.g. high availability, sensitive systems, production systems be excluded from the penetration testing activities?

ANSWER: Not relevant.

93. Will any portion of the testing need to be conducted after business hours? If so, which portion specifically: External Network Penetration Testing, Internal Network Testing, Wireless Penetration Testing, Web Application Penetration Testing?

ANSWER: See response to question 68.

94. Does analysis and reporting need to be conducted on site?

ANSWER: No. All information is proprietary, confidential and appropriately protected.

95. Will one assessment report covering all activities be sufficient, or will independent reports be required? If so, please indicate how many reports and for what portions of the assessment activities e.g. External Network Penetration Testing, Internal Network Testing, Wireless Penetration Testing, Web Application Penetration Testing?

ANSWER: See SOW Section 7 DELIVERABLES for reporting requirements.

96. Can MWAA confirm that the resumes do not count towards the 25 page limit?

ANSWER: Resumes may be presented as part of an exhibit which is not included in the 25 page limit.

97. Does MWAA host all websites that will be examined for this testing?

ANSWER: Yes.

98. Which web site would you like to assess?

ANSWER: This information will be provided to the successful offeror after contract award.

99. How many pages?

ANSWER: Not relevant.

100. Are some of these pages dynamically generated from a subset of core pages?

ANSWER: Not relevant.

101. If so, how many core pages

ANSWER: Not relevant.

102. Does the application require any client side applications If so, please list.

ANSWER: Not relevant.

103. Are there different user levels. If so, how many

ANSWER: Not relevant.

104. If there are different user levels, do you want data integrity verified between different user levels.

ANSWER: Not relevant.

105. Do you want us to make sure one level of logon cannot access information intended for another level. How many levels tested?.

ANSWER: Not relevant.

106. Is the application Internet and or externally accessible.

ANSWER: Externally.

107. Do you want black-box (unauthenticated) or white-box (authenticated) testing?

ANSWER: Black box. See answer to question 38.

108. Please expand on what you envision the test and verify the security setup and confirmation of internal IT infrastructure bullet in the RFP.

ANSWER: Testing activities will evaluate the core infrastructure such as switches, routers, etc to ensure proper configuration.

109. How many IP addresses total are in scope for internal testing? Approximately how many of those IP addresses are assigned and or active?

ANSWER: See response to question 38. There are approximately 4,000 active nodes.

110. How many external IP addresses are in scope in total for external testing? Approximately how many of those IP addresses are assigned and or active?

ANSWER: See response to question 38. 900 registered with 92 in use.

111. How many web applications in total are in scope?

ANSWER: Approximately 10.

112. Are all of the applications available from the Internet?

ANSWER: Yes.

113. Does the Authority want configuration level review of devices and operating systems? If so, what platforms and OSs are in scope.

ANSWER: Not relevant.

114. Does the Authority want network architecture level review to evaluate any security improvement possibilities in the architecture? If so, how many sites are in scope

ANSWER: Not relevant.