Clear Form

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA
SCHOOL BOARD ADMINISTRATION BUILDING
Procurement Management Services
1450 N.E. 2nd Avenue, Room 650
Miami, FL 33132

Direct All Inquiries To
Procurement Management Services

Buyer's Name: Charisma Montfort

PHONE: (305) 995- 2364

Email: cmontfort@dadeschools.net

TDD PHONE: (305) 995-2400

BID/RFP ADDENDUM

Date: 2/8/2022

Addendum No. 2

BID/RFP No. RFP-21-034-CM BID/RFP TITLE: Network Security Assessment, Testing, and Consultation Servi

This addendum modifies the conditions of the above-referenced BID/RFP as follows:

Please see attached responses to submitted questions.

The deadline for this solicitation has been extended to Tuesday, February 22, 2022.

All other terms and conditions apply.

All information, specifications terms, and conditions for the above-referenced BID/RFP, are included on the document posted on the Procurement Management website at http://procurement.dadeschools.net

The attached pages containing clarifications, additional information and requirements constitute an integral part of the referenced bid. If your bid/proposal has not been submitted, substitute the pages marked REVISED and mail your entire bid/proposal package.

I acknowledge receipt of Addendum Number ___________

PLEASE NOTE: If your firm has forwarded a copy of this bid/proposal to another vendor, it is your responsibility to forward him/her a copy of this addendum.

(PLEASE TYPE OR PRINT BELOW)

LEGAL NAME OF BIDDER: ______________________________

MAILING ADDRESS: ______________________________

CITY, STATE ZIP CODE: ______________________________

TELEPHONE NUMBER: ____________ E-MAIL ____________ FAX # ____________

BY: SIGNATURE (Manual): ______________________________
OF AUTHORIZED REPRESENTATIVE

NAME (Typed): ____________________ TITLE: ____________________
OF AUTHORIZED REPRESENTATIVE

RFP# 21-034-CM - Network Security Assessment, Testing, and Consultation Services – Q&A

1. How many of the 476 schools are in scope for this project ?
   ANSWER: All locations (including schools and administrative/support sites) are potentially in scope

2. Regarding the Comprehensive Risk Assessment, is it necessary to inspect/examine every facility or can some serve as model for others with respect to networking, wifi, physical security etc. ?
   ANSWER: A sample of locations should suffice; sites will be selected by Management and Compliance Audits

3. For years 2 and 3 for District-wide IT Risk Assessment: "Reduced/Limited". What % estimate of Comprehensive Risk Assessment would this be ? For example: Years 2 and 3 are estimated to require X% of Comprehensive work effort in each year.
   ANSWER: This response should be dependent on potential environment changes during or after initial risk assessment and/or any identified gaps or areas of concern that may require additional attention

4. What are the estimated number of:
   - External IPs for Penetration Testing ?
   - Internal IPs for Penetration Testing ?
   - Wireless network for Penetration Testing ?
   - Physical facilities for Penetration Testing (i.e. Red Teaming) ?
   - External applications for Penetration Testing ?

   ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

5. Regarding "Consultation" and the "ability to use the firm", should this be understood to include incident response and/or digital forensics ?
   ANSWER: No

6. Regarding "Consultation" and the "ability to use the firm", is remote consultation acceptable ?
   ANSWER: Yes

7. With respect to application security testing (i.e. application pen-testing), will there be testing instances of these applications available, or must testing be done on production systems ?
   ANSWER: Testing will be performed on production systems.

8. "SECTION - 4.2.2 – SCOPE OF SERVICES
   "What is the overall application landscape? Also please provide the followings:
   #Number of business critical applications, servers, network devices
   #Number of Web Applications and technology stack
   #Number of Others (if any, please specify the type of applications e.g.. ERP/COTS etc)"

   ANSWER:

   In terms of District infrastructure quantities and other general information:

Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

In-scope servers: 0-4,000

In-scope endpoints/workstations: 0-500,000

9. "SECTION - 4.2.2 – SCOPE OF SERVICES
Where are these applications of Customer deployed :- on Prem or on Cloud.? Also mention the scanning frequency for SAST, DAST for the existing application if any?

    ANSWER: District may have some cloud presence; however, security assessment of these may be limited pending agreements with cloud providers: AWS, Azure/O365; engagement for penetration testing should not take into consideration scanning frequencies or any other assessment measures. Awarded firm will be responsible for all relevant testing.

10. "SECTION - 4.2.2 – SCOPE OF SERVICES
What is the Pen Testing approach currently in-place? Is there any specific SSD(Secure Software Delivery) framework implemented? Please provide the detail expectations.

    ANSWER: Two penetration tests have been conducted, one in each of the last two fiscal years. Going forward, a penetration test is planned to be conducted annually.

11. SECTION - 4.2.2 – SCOPE OF SERVICES Please provide details of "Limited or comprehensive testing of a single or multiple domains (minimum of 2 domains per year)". Do we have any roadmap for this? Will help to map required skillset and to plan well accordingly.

    ANSWER: Scope of penetration testing and domains to be tested will be determined in collaboration with the awarded vendor and OMCA.

12. "SECTION - 4.2.2 – SCOPE OF SERVICES - What are the detail activities to be expected under Physical Penetration Testing? Please specify on the number of sites that needs to be Pen tested Physically
ANSWER: Testing of security measures while on-prem; there is no expectation that an awarded vendor perform a physical breach or test physical security of a site. Assessment of technical security measures coupled with observations of physical security concerns should suffice.

13. "SECTION - 4.2.2 – SCOPE OF SERVICES - Please outline the security tools and other technologies, SSD framework currently used in Vulnerability Management(VM) process at Miami-Dade County. Are we expected to leverage these tools for conducting the PT assessment?

    ANSWER: Scope of penetration testing and domains to be tested will be determined in collaboration with the awarded vendor and OMCA.

14. "SECTION - 4.2.2 – SCOPE OF SERVICES - A. District-wide Information Technology Risk Assessment:" Could you please elaborate on what will be covered in scope (application, infra, processes etc.) for Comprehensive assessment?
ANSWER: Risk assessment scope is flexible but may include application, infra, processes etc.

15. SECTION - 4.2.2 – SCOPE OF SERVICES SECTION - 4.2.2 – SCOPE OF SERVICES A. District-wide Information Technology Risk Assessment:" Will the Comprehensive assessment be done one time or is a continuous process to be carried out across 12 months?

    ANSWER: Comprehensive assessment to be performed once during year 1.

16. Security Review Process What will be scope for Reduced/Limited and District-wide Assessment? **ANSWER: Year 1 comprehensive risk assessment is full scope. Reduced/Limited for years 2 and 3 are flexible and scope will be dependent upon the results of year 1 assessment and dependent upon the status of implemented mitigation.**

17. "SECTION - 4.2.2 – SCOPE OF SERVICES - C. On-demand services:" What is the expected scope for Consultation?
    ANSWER: Consultation is expected to be delivered via telephone or email.

18. Security Review Process"Please let us know if any of below activities will be expected in the scope of work under Consultation:
    A) Risk Assessments on process/application - Review/update existing risk methodology, Review/update risk assessment questionnaire, conduct risk assessment, **YES**

    B) Third-party risk assessment - Aid with vendor categorization & Conduct risk classification assessment, Review/update vendor risk assessment questionnaire and **NO**

    C) Arriving at the KPI measurement, metric formulation and tracking **NO**

    D) Security Awareness - to aid with communication, newsletter and new topis on security updates"

    ANSWER: Not expected as a function of this engagement but would be welcomed if provided.

19. SECTION 8 – PROPOSAL PRICING Have you defined any pricing template Excel spreadsheet for this RFP? If not, then how are you planning to derive the total amount from different pricing formats and compare the same during evaluation? ‘

    ANSWER: No, there is no standard pricing proposal. The Selection Committee will review all submitted proposals and make a determination in the best interest of the District.

20. SECTION 8 – PROPOSAL PRICING We understand that the information in this RFP is to be utilized solely for preparing the proposal response to this RFP and does not constitute a commitment by the District to procure any product in any volume. In that case are you expecting catalog pricing for all requested services (Penetration Testing, Technology Risk Assessment, and Consulting etc.)? If not, then could you please let us know the expected pricing model for all security services - ‘Manage service’, ‘Time & Material’ etc.?

    ANSWER: Please see response to Question 19.

21. SECTION - 4.2.4 – ADDITIONAL REQUIREMENTS Do you have preference on service delivery location?

ANSWER: Remote conduction of services is satisfactory in most cases. On premises delivery as needed or required.

22. Should we be registered as Vendors to Miami Dade to submit the bid? Or is registration on DemandStar sufficient?

    ANSWER: Registration is not a requirement to submit to this bid, however, vendor registration will be required upon award.

23. Section 4.2.4, F It is mentioned that "Contractor staff conducting any testing, evaluation, review, or reporting must originate from within the United States." Does that mean all services should be delivered from USA only?

    ANSWER: Yes. As per M-DCPS policy, any and all information belonging or pertaining to the District should be hosted within the continental United States of America. Vendors from other countries who wish to engage with M-DCPS must have a presence that meets this requirement (i.e., an Amazon tenant hosted within the continental United States) and must attest that no District information will be hosted or presented outside of this environment.

24. "SECTION - 4.2.2 – SCOPE OF SERVICES | B. Penetration Testing - Please elaborate (Volume and Detailed activities) on the Domains: namely External, Internal, Wireless, Physical, Application, etc. that need to be penetrated
    ANSWER:

    Over 400 locations in disparate metropolitan areas.

    Environment is primarily Windows OS with some potential Linux and Mac deployment.

    District may have some cloud presence; however, security assessment of these may be limited pending agreements with cloud providers: AWS, Azure/O365

    District utilizes industry-standard antivirus solution(s)

    Enterprise solutions include an SAP environment

    In terms of District infrastructure quantities and other general information:

    Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

    In-scope servers: 0-4,000

    In-scope endpoints/workstations: 0-500,000

25. How many vendors were specifically invited to bid on this RFP? Who were those vendors? Has Miami-Dade received any vendor presentations relating to Cyber Security prior to the release of the RFP and cone of silence? If so, when and which vendor(s)

    ANSWER: While the District has had cybersecurity-related presentations from other vendors prior to this RFP, that information will not be disclosed at this time and should not be considered as a material concern for this RFP and/or subsequent engagement.

26. D. Proposer(s) must certify that they will not perform other testing, consulting, or sale of products or services to M-DCPS while contracted with the Office of Management and Compliance Audits (OMCA).
    - If we use a reseller for product sales and bid direct will this be allowed?

    Answer: No. This will not be allowed.

27. There shall be NO subcontracting for any of the services on this solicitation. Awarded vendor(s) shall ensure all personnel performing work under this contract are under direct employment of the awarded vendor(s).

    - If at any time services fall outside of scope can this be adjusted to allow subcontracting if under the awarded vendors badge?

    No. Subcontracting is not allowed.

28. Page 3 of the RFP states proposers must provide a performance bond, is this intended for this type of service?

    ANSWER: Please be advised that the information on page 3 is standard boiler language and not applicable in the case of this RFP.

29. Please provide more clarification on the Status Verification Section on page 6 of the RFP.

    Answer: For more information, please refer to State of Florida Executive Order 13465.

30. In Section 6.2 – Response Format on page 20 of the RFP requests proposers include Exhibit 1 in Section 1, Cover Page, of the proposer's proposal. Additionally, on page 21, Section 10, Required Forms & Exhibits, requests prospers include Exhibits 1 through 17 "as part of this proposal." Does the School Board want proposers to include Exhibit 1 in both Section 1 and Section 10 of their proposal?

    ANSWER: Inclusion of Exhibit 1 in one section is sufficient.

31. Does M-DCPS want proposers to include all copies of Exhibit 6 - Proposer Experience Form being provided in both Section 7 and Section 10 of their proposal?

    ANSWER: Inclusion in one section is sufficient.

32. Where would M-DCPS like Exhibit 9 to be included if there is no "outside" to be attached to?

    ANSWER: Please see response to Question 31.

33. Does M-DCPS want proposers to just include Exhibit 9 - Proposal Submittal Receipt Form in their proposal in addition to being attached to the outside of the proposer's response? This is for clarification as Section 10, Required Forms and Exhibits, on page 21 states that Exhibits 1 through 17 of the RFP should be included with the proposal.

    ANSWER: If submitting a hard copy, please place Exhibit 9 on the outside of your package.

34. What should proposers include for Exhibit 12- Instructions for Certification as this

Exhibit is just a list of instructions and has no place for the proposer to sign? This is for clarification as Section 10, Required Forms and Exhibits, on page 21 states that Exhibits 1 through 17 of the RFP should be included with the proposal.

ANSWER: This form does not require signature or notarization.

35. Does M-DCPS want proposers to just include Exhibit 15 - Mailing Label in their proposal? This is for clarification as Section 10, Required Forms and Exhibits, on page 21 states that Exhibits 1 through 17 of the RFP should be included with the proposal.

    ANSWER: If submitting a hard copy, please place Exhibit 15 on the outside of your package.

36. Does M-DCPS want proposers to include Exhibit 16 - Statement of "No Response" with their proposal even if they are indeed responding? This is for clarification as Section 10, Required Forms and Exhibits, on page 21 states that Exhibits 1 through 17 of the RFP should be included with the proposal.

    ANSWER: No.

37. Does M-DCPS want proposers to include Exhibit 17 – Proposed Contract Agreement Draft on pages 50 through 58 in their proposal, or is it only for reference? This is for clarification as Section 10, Required Forms and Exhibits, on page 21 states that Exhibits 1 through 17 of the RFP should be included with the proposal.

    ANSWER: Exhibit 17 is only for reference. Please identify any contract exceptions you might have.

38. Just to confirm what was written on page 19 of this RFP: proposers can submit proposals by submitting to Demandstar without mailing a hardcopy, correct?

    ANSWER: Correct.

39. What does a comprehensive assessment consist of? I.e. penetration test with risk assessment etc?

    Answer: Penetration testing will not be included as part of the comprehensive Risk Assessment.

40. How many public IPs and appliances are in scope of the External Assessment?

    ANSWER:

    Any information REQUIRED to perform testing will be provided as necessary.

    In terms of District infrastructure quantities and other general information:

    Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

    In-scope servers: 0-4,000

    In-scope endpoints/workstations: 0-500,000

41. What are the make of the edge devices being used?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

42. Under section 4.2.4 subsection I:
“Proposer shall utilize appropriate testing and assessment standards. The primary standards used should be the most recent revision of the National Institute of Standards and Technology (NIST) Publication 800-53. Primary PEN test criteria should be the Penetration Testing Execution Standard as described at http://www.pentest-standard.org.“ Is it meant to call out NIST 800-53 or are you referring to NIST 800-115?

ANSWER: NIST 800-115 is incorporated into NIST 800-53 R5 by reference.

43. What is the business requirement for this penetration test? a. This is required by a regulatory audit or standard?

ANSWER: NO

44. Proactive internal decision to determine all weaknesses?

ANSWER: YES

45. For example, is the driver for this to comply with an audit requirement, or are you seeking to proactively evaluate the security in your environment?

ANSWER: The OMCA is proactively seeking evaluation and testing to identify and mitigate weaknesses that may impact the mission of the District.

46. How many IP addresses and/or applications are included in scope for this testing?
Please list them, including multiple sites, etc

ANSWER: Over 400 locations in disparate metropolitan areas.

Environment is primarily Windows OS with some potential Linux and Mac deployment.

District may have some cloud presence; however, security assessment of these may be limited pending agreements with cloud providers: AWS, Azure/O365

Enterprise solutions include an SAP environment

In terms of District infrastructure quantities and other general information:

Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

In-scope servers: 0-4,000

In-scope endpoints/workstations: 0-500,000

47. What are the objectives?
i. Map out vulnerabilities **Yes**

ii. Demonstrate that the vulnerabilities exist **Yes**

iii. Test the Incident Response and Processes **Yes, if applicable**

48. Actual exploitation of a vulnerability in a network, system, or application. Obtain privileged access, exploit buffer overflows, SQL injection attacks, etc. This level of test would carry out the exploitation of a weakness and can impact system availability.
ANSWER: Testing should avoid impacting system availability or integrity whenever possible; identification of vulnerable assets without an actual exploit should suffice.

v. Protection of specific resource **This assessment is for the District at-large**

vi. Other

49. What are the times penetration testing (scanning, exploiting) should occur?

ANSWER: To reduce the potential impact of penetration testing on the production environment, there will be specific testing windows provided by the OMCA. Conversely, blackout periods where no testing can be performed will also be provided by the OMCA. However, it may be possible to schedule some testing during non-business hours if necessary or beneficial.

50. Do you have any documentation associated with your network? I.e. network diagrams.
ANSWER: Yes.

51. How many public IP addresses?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

52. How many public domain names?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

53. How many users are there?
ANSWER: 0-750,000 potential users

54. What is the domain functional level?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

55. How many domain controllers are there?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

56. How many sites are there?
ANSWER: 400 sites in disparate metropolitan locations

57. Are there any Trusts in place with other forests?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

58. What operating systems are in the environment?
ANSWER: Environment is primarily Windows OS with some potential Linux and Mac deployment.

59. How many total Machines are in the environment?
ANSWER: Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

In-scope servers: **0-4,000**

In-scope endpoints/workstations: **0-500,000**

60. What is the breakout of Servers to workstations?
ANSWERS:

In-scope servers: **0-4,000**

In-scope endpoints/workstations: **0-500,000**

61. Are there any sensitive networks, if so what are they? I.e. PCI, SCADA, HIPAA

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

62. Are there any key objectives or specific systems/networks you would like to focus on?

ANSWER: The District's entire network and infrastructure is in scope for both assessment and testing, as guided by the OMCA.

63. What are your major compliances or regulations?

ANSWER: Applicable federal, state, and local laws and regulations.

64. What are the times testing (scanning, exploiting) should occur?

ANSWER: To reduce the potential impact of penetration testing on the production environment, there will be specific testing windows provided by the OMCA. Conversely, blackout periods where no testing can be performed will also be provided by the OMCA. However, it may be possible to schedule some testing during non-business hours if necessary or beneficial.

65. Are there network designs that can be provided for evaluation?

ANSWER: Yes. Any information REQUIRED to perform testing will be provided as necessary.

66. For Wireless Assessments - How many access points are in scope of this assessment?

ANSWER: Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

67. Are there any wireless controllers in scope of the assessment?
ANSWER: Yes, the District has wireless controllers that are included in scope.

68. What is the make of the access points and controllers?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

69. Are client level exploits in scope of the assessment?

ANSWER: YES

70. Do you have any documentation on the wireless environment? Such as network maps, physical maps, mac address listings etc.

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

71. For Physical Assessments - What is the scope of the physical assessment?
ANSWER: Assessment of technical security measures coupled with observations of physical security concerns should suffice.

72. Are you looking to test physical bypasses such as picking locks or bypassing cameras?

ANSWER: No

73. Are you looking for social engineering? Phishing, Vishing, Impersonation

ANSWER: Possibly, as guided by the OMCA.

74. Are you looking to test the responsiveness of emergency response? I.e. how long does it takes police to arrive on site?

ANSWER: No

75. For Web Application Assessments - How many web applications are in scope?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

76. From 1 being not at all to 5 being entirely dynamic reliant on other dynamic applications, how dynamic is your application?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

77. What language is your application written in?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

78. Will source code be provided?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

79. Will a demonstration be provided?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

80. SECTION - 4.2.4.D - Can the team elaborate the scope of this? If a company is currently providing M-DCPS products and services via an existing contract, does this mean they cannot work on the OMCA project under 21-034-CM?
Or, is this strictly scoped to Cybersecurity projects with the district where the vendor cannot work with M-CDPS on Cybersecurity while they are working with OMCA?

81. External Scope – the following will tailor pricing proposal to M-DCPS
How many active Internet facing IP Addresses to be tested?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

82. How many Number of Domain Names owned/registered (DNS)?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

83. How many servers to be tested (this number may change) tested?
ANSWER: In-scope servers: 0-4,000 • How many workstations estimated? In-scope endpoints/workstations: 0-500,000
- Number of other network devices to be tested?
  - **Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices**
- Number of Microsoft Active Directories to be tested? **Any information REQUIRED to perform testing will be provided as necessary.**
- Number of wireless physical locations to be tested? **To be determined by the OMCA.**

84. Will there be "capture the flag" assessments needed – for example – ERP Admin Access, Access to CIO's email, etc?
ANSWER: NO

85. Application Penetration Test - We do an unauthenticated scan by default, would you like us to do an authenticated scan as well?

ANSWER: If penetration testing yields authentication credentials, yes.

86. If so, how many authenticated scans will be needed (Typical test is for one unauthenticated and one general authenticated user) - Value entered should be total of unauthenticated and authenticated scans to be performed.
ANSWER: If penetration testing yields authentication credentials, yes.

87. Is there a Web application firewall (WAF) in place **Any information REQUIRED to perform testing will be provided as necessary.** Are APIs/AJAX/Service calls being used and need to be tested? If so, how many?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

88. Is a Code review of the application desired
ANSWER: Potentially yes, as guided by the OMCA.

89. What language(s) is it written in (e.g. .php, java, .Net, etc…)
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

90. What language is the back end database?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

91. Would The School Board of Miami-Dade County, Florida, accept the use of offshore resources along with local resources to support the project? All resources would be from the same vendor.

ANSWER: No. As per M-DCPS policy, any and all information belonging or pertaining to the District should be hosted within the continental United States of America. Vendors from other countries who wish to engage with M-DCPS must have a presence that meets this requirement (i.e., an Amazon tenant hosted within the continental United States) and must attest that no District information will be hosted or presented outside of this environment.

92. Is there a budget for this project, and if so, can you disclose what that is?

    ANSWER: Budget has not been finalized. Estimated budget: $300,000 to 600,000

93. Regarding Section 1, Section I Preparation of Proposals, #2: it mentions requiring "original manual signatures" for the forms. If we are submitting electronically via upload, are electronic or scanned signatures acceptable?

    ANSWER: Yes.

94. What portion, if any, of the work for this project can be conducted remotely?
    ANSWER: Penetration testing can be conducted remotely if possible within the scope of required functions; however, the District may be unable to accommodate certain remote functions if the integrity of District security measures may be compromised externally as a result. Risk assessment should largely be conducted on prem.

95. Could you provide additional information regarding the size of the internal/external environments and how many IP addresses will be part of the penetration testing? How many applications are in-scope? How many wireless access points and SSIDs are in scope?

    ANSWER:

    Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

    In-scope servers: 0-4,000

    In-scope endpoints/workstations: 0-500,000

96. Is the physical assessment to include social engineering? If so, how many employees will need to be assessed?

    ANSWER: Possibly, as guided by the OMCA.

97. Request clarification to Section 4.2.4 Additional Requirements (D). If our company has ANY existing business with M-DCPS today or during the contract period, we would be excluded from the potential of an award, correct?

    ANSWER: Yes, you would be excluded.

98. Are there PCI DSS requirements for Authenticated Scan Vendor (ASV)? Are there any other compliance requirements for PCI, NIST and/or HIPAA ?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

99. How many “live” IP addresses are in-scope that are publicly accessible (i.e.: facing the Internet)? A “Live” IP address is one that is assigned to a device.

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

100. How many “live” IP addresses are in-scope for scanning inside the organization that are not publicly accessible? A “Live” IP address is one that is assigned to a device.

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

101. If scanning within the private network is desired, can all in-scope IP addresses and web applications be reached from a single point in the network? If not, how many locations would scanning need to occur from to reach all in-scope IP’s / Web Apps?

ANSWER: On-prem security measures may prevent this function; in-scope functions will be coordinated with OMCA and ITS.

102. How many Web Applications would be in-scope for testing?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

103. How large is the IP space to be assessed (i.e., range size, how many class Cs, Class Bs, etc.)?

ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

104. How may hosts are in scope as part of this assessment?

ANSWER: In terms of District infrastructure quantities and other general information:

Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

In-scope servers: 0-4,000

In-scope endpoints/workstations: 0-500,000

105. Are any systems or devices in scope hosted by a third party?

ANSWER: District may have some cloud presence; however, security assessment of these may be limited pending agreements with cloud providers: AWS, Azure/O365

106. If IDS/IPS systems are in place, is the assessment also intended to test the responsiveness during this assessment, or will AT&T Cybersecurity Consulting systems be configured as exceptions in the IDS/IPS?

ANSWER: Yes, responsiveness is in scope. Any information REQUIRED to perform testing will be provided as necessary. The District may be unable to accommodate certain remote functions if the integrity of District security measures may be compromised externally as a result.

107. Can a network diagram be provided?
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

108. For Penetration Testing, how many databases need to be reviewed? (each instance counts as a separate database)
ANSWER: Any information REQUIRED to perform testing will be provided as necessary.

109. RFP referenced 37,830 employees, however on the call we think we heard 45,000. Can you confirm which figure is correct?
ANSWER: As of January 2022, there are 39,095 full and part time employees.

110. When would the addendum be posted online with the answer's to our inquires?
ANSWER: This addendum addresses all submitted questions.

111. Can the bid's response be extended to February 28th , 2022?
ANSWER: The deadline for this solicitation is Tuesday, February 15, 2022 at 1pm.

112. Could more elaboration surrounding the assets be assessed, such as an approximate number of endpoints to be assessed and the number of servers and external IPs?
Switches, routers, firewalls, Intrusion Prevention/Detection Systems, wireless controllers, access points, etc.: 0-40,000 devices

In-scope servers: 0-4,000

In-scope endpoints/workstations: 0-500,000

113. What level of physical penetration testing is expected? Is the contractor expected to assess the physical security of sites, or is "breaking in" required to assess the response of on-site personnel? If "breaking in" is needed, will security personnel be notified ahead of time to reduce actual risk to on-site assessor/s?

ANSWER: Testing of security measures while on-prem; there is no expectation that an awarded vendor perform a physical breach or test physical security of a site. Assessment of technical security measures coupled with observations of physical security concerns should suffice. At no point should awarded vendor engage in behaviors that may result in any risk to the assessor(s).