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: Vanessa Flores
PHONE: (305) 995- 2646
Email: vflores@dadeschools.net
TDD PHONE: (305) 995-2400

BID/RFP ADDENDUM

Date: 05/04/2022

Addendum No. 1

BID/RFP No. RFP-21-009-VF BID/RFP TITLE: ESSER NIST Cybersecurity Services

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

The attached document provides answers to questions received. In addition, Revised Section 8 - Proposal Pricing has been included with this addendum.

All other terms and conditions of the RFP will remain the same.

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 1

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

REVISED SECTION 8 – PROPOSAL PRICING

(Signature required at the end of this Section)

Proposer must complete this Section in its entirety and may supplement this section with additional pages as to provide the District with a more detailed breakdown, backup and/or options of related costs associated with the services being solicited in this RFP.

Proposer must itemize and detail all chargeable fees to perform all elements of this RFP identified in **Section 4,** Scope of Services.

NIST Cybersecurity Service	Estimated Number of Hours to Perform Service	Hourly Rate to Perform Service
Hourly Rate to provide Compromise Assessment services as specified in Section 4, Scope of Services	_____	**$**_____
Hourly Rate to provide Incident Response services as specified in Section 4, Scope of Services.	_____	**$**_____
Hourly Rate to provide Managed Detection and Response (MDR) including a tabletop exercise resulting in a runbook service as specified in Section 4, Scope of Services.	_____	**$**_____
Hourly Rate to provide Vulnerability Assessment services as specified in Section 4, Scope of Services.	_____	**$**_____
Hourly Rate to provide Digital Forensics services as specified in Section 4, Scope of Services.	_____	**$**_____
Hourly Rate to provide Penetration Testing services as specified in Section 4, Scope of Services.	_____	**$**_____
Hourly Rate to provide Gap Analysis services as specified in Section 4, Scope of Services.	_____	**$**_____

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.

The Proposer shall offer all elements of this RFP and meet all service requirements and specifications listed within Section 4 - Scope of Services, including but not limited to all costs associated with the performance of these services, including labor, materials, transportation, training, maintenance, fees, etc.

THE EXECUTION OF THIS FORM CONSTITUTES THE UNEQUIVOCAL OFFER OF THE PROPOSER TO BE BOUND BY THE TERMS OF ITS PROPOSAL. FAILURE TO SIGN THIS PRICE PROPOSAL WHERE INDICATED BELOW BY AN AUTHORIZED REPRESENTATIVE OR PROVIDE THE FORM AS PRESENTED MAY RENDER THE PROPOSER NON-RESPONSIVE.

_____ _____

Signature of Proposer's Authorized Representative *Title*

_____ _____

Printed Name: *Date:*

Request for Proposals
RFP-21-009-VF
ESSER NIST Cybersecurity Services

ADDENDUM NO. 1

QUESTIONS AND ANSWERS:

Q1: Is there a max bill rate for this position?

A1: No

Q2: Was the previous assessment NIST NCF-based?

A2: The District is unaware of the standards utilized.

Q3: What control families were used to inform the assessment? E.g. 800-53v4, ISO27001, CIS

A3: The District is unaware of the standards utilized.

Q4: Does the school system have any preference for certain control families for risk assessments?

A4: The District is would like to test for NIST 800-53 and ISO 27001.

Q5: Is there an expectation of being onsite for incident response services or can it be offered remotely?

A5: The Web application and Network Assessment component can be remote; any wireless pen test will most likely need to be on site.

Q6: Are there any requirements for data to reside within the United States?

A6: Yes, all data should remain within the continental USA only.

Q7: For the MDR service, can it be a SaaS?

A7: It can be, however it should also abide by SOC 1,2, NIST and ISO 27001 compliance. Additionally, data needs to reside in the USA only.

Q8: External Network Vulnerability Assessment /Penetration Testing. Which type of pen test approach is requested? Please select a testing approach from: black box (no knowledge) testing, gray box (some knowledge), or white box (complete knowledge)? Each has its benefits and time considerations and costs. (We would recommend the Gray Box approach for cost and efficiency benefits).

A8: While this is not a “penetration testing” RFP, per se, as a potential service available within this engagement, limited penetration testing scope would be determined based on departmental needs. Testing may be limited to a single system or a much broader scope. Engagement would likely be gray or white box.

Q9: External Network Vulnerability Assessment /Penetration Testing. Total number of public facing / external network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).

A9: While this is not a “penetration testing” RFP, per se, as a potential service available within this engagement, limited penetration testing may encompass a range of external IP addresses. For pricing purposes, please provide a quote for 0-100 IPs, 101-499 IPs, 500-1000 IPs.

Q10: External Network Vulnerability Assessment /Penetration Testing. Number of Web based applications/ services to test, if any (dynamic pieces of websites that users or other application authenticate to – client portal, sales quote system).

A10: Please provide pricing for the following ranges for application testing: 0-10 and 11-40 applications (authenticated testing) and 0-5 and 1-40 applications (unauthenticated testing).

Q11: External Network Vulnerability Assessment /Penetration Testing. VPN, Terminal Services, Remote Desktop, FTP, and other remote services to be tested?

A11: All of these services could potentially be in scope should the District opt to utilize external vulnerability assessment/penetration testing services via this engagement.

Q12: External Network Vulnerability Assessment /Penetration Testing. Is an objective of this test to also assess the organization’s intrusion detection capabilities?

A12: The District welcomes the opportunity to tune our system to better detect threats.

Q13: External Network Vulnerability Assessment /Penetration Testing. How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?

A13: Provide a cost associated with each subsequent level of testing and validation or deeper access testing.

Q14: External Network Vulnerability Assessment /Penetration Testing. Are any of the external systems hosted by a third-party provider?

A14: No third-party systems will be directly tested or in-scope for testing.

Q15: Internal Network Vulnerability Assessment /Penetration Testing. Total number of internal network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).

A15: For pricing purposes, please provide a quote for 0-1000 IPs, 1001-4999 IPs, 5000-10000 IPs, etc., if there is a price variance for additional testing volume.

Q16: Internal Network Vulnerability Assessment /Penetration Testing. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?

A16: Provide a cost associated with each subsequent level of testing and validation or deeper access testing.

Q17: Internal Network Vulnerability Assessment /Penetration Testing. Are internal web based applications / services in scope, if so, please provide an indication as to the anticipated number of web based applications/services that may need to be assessed.

A17: Please provide pricing for the following ranges for application testing: 0-10 and 11-40 applications (authenticated testing) and 0-5 and 1-40 applications (unauthenticated testing).

Q18: Internal Network Vulnerability Assessment /Penetration Testing. Can remote internal networks be scanned via a primary location or would it be necessary to perform field visits to each in-scope location?

A18: Some remote scanning from within the network may be possible depending on the necessary activities and scope of work.

Q19: Who is the project's sponsor?

A19: Miami-Dade County Public Schools, Information Technology Services Department

Q20: How is this project being funded?

A20: ESSER funds

Q21: What is the budget allocated for this project?

A21: $160,000

Q22: Is there an expected completion date? If so, what is it?

A22: There is no expected completion date; the intent of this RFP is to secure services on an as-needed basis to perform a broad range of cybersecurity and related functions.

Q23: Will CoF select just one vendor to provide these services?

A23: The District may select multiple vendors for these services.

Q24: Did CoF have an outside firm help in preparing the RFP? If yes, will that firm be allowed to bid on this project

A24: No outside firm assisted with the preparation of the RFP.

Q25: Type of Security Monitoring Service(s); what is the client's expectation/requirement of the service.

1. **Monitoring Triage & Notification**
    a. **24 x 7 | off-hours | hybrid | custom monitoring coverage**
2. **Log Collection & Storage (some level of collection/storage will be required to support Analysis and Response)**
3. **Vulnerability Identification (Scanning)**
4. **Intrusion Detection**
    a. **Network / Host**
5. **Asset Identification**
6. **Compliance Reporting**
7. **Endpoint Detection & Response (workstations)**
8. **Cloud Services Monitoring**
9. **Server & Services Availability Monitoring & Alerts**
10. **Security Response and Remediation Support**

A25: Any/all of these services may be within scope.

Q26: Number of Firewalls and each make/model?

A26: Information will be shared as necessary once the solicitation is awarded.

Q27: Any Web Application Firewalls?

A27: Information will be shared as necessary once the solicitation is awarded.

Q28: DNS Server (Microsoft, BIND, etc.)?

A28: Information will be shared as necessary once the solicitation is awarded.

Q29: Any Netflow capabilities?

A29: Information will be shared as necessary once the solicitation is awarded.

Q30: Number of Infrastructure devices (routers, switches, etc…) and each make/model?

A30: Information will be shared as necessary once the solicitation is awarded.

Q31: Number of Servers and each make/model/OS?

A31: Information will be shared as necessary once the solicitation is awarded.

Q32: Number of Active Directory or Ldap Servers?

A32: Information will be shared as necessary once the solicitation is awarded.

Q33: Number of and any specific files, if file integrity monitoring is an objective

A33: Information will be shared as necessary once the solicitation is awarded.

Q34: Number of endpoints (workstations) and each make/model/OS

A34: Information will be shared as necessary once the solicitation is awarded.

Q35: Does the Client have a virtual environment that can host the SIEM sensor virtual image?

A35: The District cannot provide a response without further clarity on this question.

Q36: Number of Virtual Services and make and model?

A36: Information will be shared as necessary once the solicitation is awarded.

Q37: What, if any, cloud environment would be in-scope (AWS, Azure, O365, etc.)?

A37: Limited O365, Azure aspects may be within scope.

Q38: Can you share your network diagrams?

A38: Information will be shared as necessary once the solicitation is awarded.

Q39: Can you share an asset inventory for in-scope devices by asset type?

A39: Information will be shared as necessary once the solicitation is awarded.

Q40: How many locations are in-scope for collection and monitoring? Are these locations reachable from a single site; are these sites independent / segmented?

A40: This is dependent upon determined/required scope of engagement; Information will be shared as necessary once the solicitation is awarded.

Q41: How many isolated network segments exist across the network?

A41: Information will be shared as necessary once the bid is awarded.

Q42: How many employees/contractors/vendors/interns have access to the network that will be monitored?

A42: 0 - 50,000 possible employees/contractors/vendors/interns; this count does not include students.

Q43: Do you know your current Events Per Second (EPS) for in-scope networks?

A43: Current Average is about 45,000 EPS.

Q44: Do you know your current number of logs to be monitored for in-scope networks?

A44: Log monitoring is currently performed in-house; review of aggregated logs may be within the scope of required services depending on the engagement.

Q45: What other security controls do you have in place (IDS, EndPoint / EDR, Proxies, etc.)?

A45: Information will be shared as necessary once the solicitation is awarded.

Q46: For user data enrichment, we typically connect to either Active Directory or an HR system to add employee name, org, supervisor, etc. to data analysis. Does your AD have additional information, Full Name, Title, Department, Supervisor, Location, etc? Alternatively, is there an HR or other system you would like us to connect with to add that information?

A46: Information will be shared as necessary once the solicitation is awarded.

Q47: Number and location of Internet ingress/egress points

A47: Information will be shared as necessary once the solicitation is awarded.

Q48: Internet Pipe size at each ingress/egress

A48: Information will be shared as necessary once the solicitation is awarded.

Q49: List of remote/branch sites if applicable

A49: Information will be shared as necessary once the solicitation is awarded.

Q50: Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?

A50: No

Q51: Specify the VLAN details how many is included in the Scope?

A51: Information will be shared as necessary once the solicitation is awarded.

Q52: Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.

A52: Approximately 400,000.

Q53: Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)?

A53: Approximately 400,000.

Q54: Can you tell the total number of endpoints you want protected?

A54: This engagement is not specifically intended to provide endpoint protection.

Q55: What's your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?

A55: 0 - 50,000 employees; less than 5% work remotely at any given time.

Q56: How much (%) of the infrastructure is in cloud?

A56: Information will be shared as necessary once the solicitation is awarded.

Q57: What is the size of the IT environment? How many physical locations?

A57: Less than 500.

Q58: What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?

A58: Information will be shared as necessary once the solicitation is awarded.

Q59: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

A59: We manage our own data center.

Q60: What is the approximate budget?

A60: $160,000

Q61: Is M-DCPS looking to implement services only, or are they seeking an EDR tool along with a 24x7 MDR service?

A61: This RFP is for services only at this time.

Q62: Does M-DCPS have an EDR tool currently installed? If so, what is it, and is it fully deployed on the endpoints in scope?

A62: Yes, we have Microsoft Defender and Cylance; additional information will be shared as necessary once the solicitation is awarded.

Q63: Can M-DCPS break down its current # of endpoints by Operating System and specify whether they are using an existing EDR on them? Is it Microsoft Defender for the Endpoint (MDE)? If so, does M-DCPS have the full license which vendor can use?

A63: The District has enterprise licensing for endpoint protection; additional information will be shared as necessary once the solicitation is awarded.

Q64: What data is being considered for ingestion into any SIEM solution that M-DCPS is considering

A64: M-DCPS currently has a SIEM solution; an alternate SIEM is not currently in scope, but assistance with evaluating data collected within the SIEM and/or leveraging existing tools may be within the scope of requested services.

Q65: Please define what "Conduct Part 121" means.

A65: This was erroneous text within the RFP. The RFP should read "Conduct NIST CFS Assessments for 5 Core Functions and 23 Categories." Please note that NIST 800-53 Moderate baseline may be substituted for NIST CSF.

Q66: Is Miami-Dade interested in ongoing services after the assessment such as monthly meetings to help prioritize, remediate and assist with the remediation of the exposure issues?

A66: Please include a cost for this service as a separate line item if there is an additional charge for ongoing services/meetings.

Q67: Does Miami-Dade have a Security Operations Center?

A67: No

Q68: Please verify if subcontracting is allowed?

A68: Subcontracting is permitted under this contract. The vendor shall be held fully responsible and liable for the supervision and performance of all work performed by subcontractors. M-DCPS shall not be responsible for resolution of disputes between the vendor and any subcontractor.

Q69: Number of endpoints?

A69: Approximately 400,000.

Q70: How many and please provide the departments that will be part of the Gap Analysis?

A70: Information Technology Services will be the primary department involved in any gap analysis.

Q71: What is the anticipated budget?

A71: $160,000

Q72: When is the desired completion date for this project for each year?

A72: Varies

Q73: Who is the incumbent for this project?

A73: There is currently no incumbent.

Q74: Are there any constraints on the project timeline?

A74: Requested services must be completed before EOY 2023.

Q75: Are there any constraints during testing?

A75: There may be student testing/assessment periods where testing will be paused to ensure that there is no interruption and potential subsequent invalidation of student assessments.

Q76: Page 3 of the RFP states proposers must provide a performance bond, which is typically used for constructing services. Does M-DCPS intend for responders to provide a performance bond for this contract?

A76: A performance bond is not required for this RFP.

Q77: Please provide more clarification on the Status Verification Section on page 6 of the RFP.

A77: Fore more information, please refer to Executive Order 13465.

Q78: On page 15 of the RFP, M-DCPS states: "In no more than ten (10) pages, the Proposer must include the following information within the submitted proposal." Is this ten-page limit applicable to the Section 6.2 – Response Format listed on page 18? I.e., is the ten-page limit for the entire proposal, or is it only relevant to the four sections listed on page 15?

A78: The ten-page limit is relevant to the items listed in Section 4.4, Items 1 through 4.

Q79: 9. Please provide more information on the Section 4.3 Services that the M-DCPS may request on an as-needed basis:
a. Compromise Assessment
b. Incident Response Service
c. Managed Detection and Response (MDR) including a tabletop exercise resulting in a runbook
d. Vulnerability Assessment
e. Digital Forensics
f. Penetration Testing

A79: Any/all of these services may be within scope for this engagement depending on District needs.

Q80: Does M-DCPS have a specific pricing sheet for the requested GAP Analysis? There is no line item for this service on the Section 8 – Proposal Pricing found on page 22 of the RFP.

A80: Please refer to Revised Section 8 posted with this addendum.

Q81: 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?

A81: The three client references on Exhibit 6 should be included within the proposal in only one section, either section will be acceptable.

Q82: Where would M-DCPS like Exhibit 9 to be included if there is no "outside" to be attached to?

A82: If Proposer is submitting a hard copy response, Exhibit 9 shall be included, however if submitting an electronic copy only Exhibit 9 does not have to be included.

Q83: 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 18 states that Exhibits 1 through 17 of the RFP must be included with the proposal.

A83: If Proposer is submitting a hard copy response, Exhibit 9 shall be included, however if submitting an electronic copy only Exhibit 9 does not have to be included.

Q84: Should proposers include Exhibit 12- Instructions for Certification in their proposal even though 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 18 states that Exhibits 1 through 17 of the RFP must be included with the proposal.

A84: Exhibit 12 does not have to be included in the Proposers response; this is for informational purposes only.

Q85: 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 18 states that Exhibits 1 through 17 of the RFP must be included with the proposal.

A85: If Proposer is submitting a hard copy, mailed response, Exhibit 15 shall be included, however if submitting an electronic copy only Exhibit 15 does not have to be included.

Q86: 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 18 states that Exhibits 1 through 17 of the RFP must be included with the proposal.

A86: Exhibit 16 does not have to be included in the Proposers response; this exhibit is only for proposers not submitting a response.

Q87: Does M-DCPS want proposers to include Exhibit 17 – Proposed Contract Agreement Draft on pages 45 through 53 in their proposal, or is it only for reference? This is for clarification as Section 10, Required Forms and Exhibits, on page 18 states that Exhibits 1 through 17 of the RFP must be included with the proposal.

A87: Exhibit 17 does not have to be included in the Proposers response; this is for informational purposes only.

Q88: Section 4.3, page 15, Might the scope of services change to align the assessment with NIST 800-53 instead of NIST CSF?

A88: NIST 800-53 Moderate baseline may be substituted for NIST CSF.

Q89: Section 4.3, page 15, Can you describe "Part 121" for vendors?

A89: This was erroneous text within the RFP. The RFP should read "Conduct NIST CFS Assessments for 5 Core Functions and 23 Categories." Please note that NIST 800-53 Moderate baseline may be substituted for NIST CSF.

Q90: Section 4.3, page 15, Will the District engage with only a single, or multiple vendors for the on-demand services?

A90: The District may select multiple vendors for this engagement.

Q91: Section 4.3, page 15, As the 4th largest school district, can the assessment be conducted from one location, or will multiple locations need to be visited, and if so, how many?

A91: Information will be shared as necessary once the solicitation is awarded.

Q92: Section 4.3, page 15, Is the focus of the assessment be an assessment of gaps against NIST CSF or a risk assessment? Or both?

A92: NIST 800-53 Moderate baseline may be substituted for NIST CSF.

Q93: Section 4.3, Does the District expect to use the "as needed" services on an annual retainer that can be "re-filled" as hours are used?

A93: Possibly

Q94: Section 4.3, Since the scope of these services cannot be known, are we able to quote an hourly fee for those services, rather than estimating the hours the work will require?

A94: Please provide a minimum estimated number of hours to provide the service requested and hourly rate.

Q95: Section 4.3, Does the District use any current tools / platforms to manage their current assessments?

A95: Information will be shared as necessary once the solicitation is awarded.

Q96: As discussed in the meeting this morning, would the School Board please update the pricing table to reflect the NIST CSF assessment and gap analysis?

A96: Please refer to Revised Section 8 posted with this addendum.

Q97: In order to price for vulnerability assessments and penetration testing, would the School Board please provide the number of:

- **Active IPS (or external)**
- **IPs or subnets that would be in scope for internal**
- **Any other information regarding the size of its IT environment that might be applicable, e.g., the number of firewalls**

A97: Information will be shared as necessary once the solicitation is awarded.

Q98: For pricing Incident Response Services and Digital Forensics, would the School Board please provide an approximate number of hours to be used as a basis for comparison between vendors, or would it be permissible to provide an hourly rate for these services? Actual hours would vary greatly based on the nature and severity of an incident.

A98: Please provide a minimum estimated number of hours to provide the service requested and hourly rate.

Q99: Regarding the NIST CSF assessment and gap analysis, would the School Board please provide the following:

- **How many enterprise applications will be in scope?**
- **How many documented IT policies and procedures currently exist?**
- **Clarification regarding the scope of the assessment and gap analysis. Will it include both an assessment of the existing cybersecurity plan and an analysis of the environment, including technical testing, or just one or the other?**

A99:

- Please see response to question 10.
- Information will be shared as necessary once the solicitation is awarded.
- May include both.

Q100: Regarding the managed detection and response services requested:

- **Can the School Board confirm that the new SIEM in place is QRadar from IBM?**
- **How the School Board would like to have the tabletop exercise delivered and to how many staff?**

A100: Yes, Qradar. Please provide potential options for tabletop exercise delivery; pricing should reflect 0-20 staff.

Q101: RFP section 4.3 identifies 6 additional services that "could" be required "as-needed." Due to the page constraints in Section 4.4, is the School Board expecting:
- **Methodologies for these services?**
- **Them to be represented in our proposal's section 6.2.6 (Re: RFP section 4.4) or is a response to Section 8 form (in our proposals 6.2.10 required forms section) all that is needed?**

A101: The ten-page limit is relevant to the items listed in Section 4.4, Items 1 through 4. Proposers are welcome to include proposed methodologies as listed in Section 6.2; itemized pricing should be included in the pricing proposal section.

Q102: On Section 4.3 the Required Services highlights the NIST CSF Gap Analysis as the primary project but the price sheet in Section 8 is requesting pricing on the possible additional services... Are you going to add a line to section 8 pricing form for the NIST Gap Analysis pricing?

A102: Yes

Q103: How many total IP addresses?

A103: Information will be shared as necessary once the solicitation is awarded.

Q104: How many servers?

A104: Information will be shared as necessary once the solicitation is awarded.

Q105: How many workstations?

A105: Information will be shared as necessary once the solicitation is awarded.

Q106: What kind of operating systems are in the environment? We would like the versions too? Example, Windows 10, Windows Server 2019, Redhat Linux, MacOs Catalina, etc....

A106: All major Windows OS's, and NOS's as well as Mac OS and some linux.

Q107: Digital Forensics - Are you using any SaaS products in scope? Example, Office 365, Google Drive, etc?

A107: Information will be shared as necessary once the solicitation is awarded.

Q108: Cloud Infrastructure - Are you using any cloud infrastructure service? Example, Google Cloud, AWS, MS Azure? If so, please describe what services are in place. Example, Servers, application work loads, etc.....

A108: Information will be shared as necessary once the solicitation is awarded.

Q109: Tabletop exercise resulting in a runbook - Do you have an existing Incident Response Plan? Do they have any documented playbooks for responding to a security incident? If so, what playbooks do you have?

A109: We do have an incident response plan; additional information will be shared as necessary once the solicitation is awarded.

Q110: Have you ever conducted a NIST Cybersecurity Framework Assessment previously?

A110: The District has not.

Q111: Please describe the maturity of your organization's Security Documentation Library.

A111: Information will be shared as necessary once the solicitation is awarded.

Q112: How in depth would you like this assessment to be? ("Tell Me", "Show Me", "Prove It". Descriptions below)
•"Tell Me" - Documentation Reviews and Stakeholder Interviews
•"Show Me" - Documentation Reviews, Stakeholder Interviews, and Selective Technical Testing / Validation
•"Prove It" - Documentation Reviews, Stakeholder Interviews, and Technical Testing of Control Design and Effectiveness

A112: Provide a cost associated with each subsequent level of testing and validation or deeper access testing.

Q113: For clarification purposes, the RFP's scope refers to a Vulnerability Assessment which is different than a Risk Assessment. Just to confirm, a Risk Assessment is not considered within the scope of this RFP each time a vulnerability assessment is mentioned. Is this correct?

A113: Correct.

Q114: RFP is awarding 10 points to MDCSP - M-DCPS-certified African American Firms – Maximum 10 points for Prime or Subcontractor . Yet the OEO site has no qualified firms. How is this requirement to be achieved? Why are all the other Minorities being discriminated?

A114: Please refer to Section 7.7 for additional information regarding how to become a certified firm with M-DCPS. Pursuant to School Board Policy 6320.02, the Goal Setting Committee reviewed the solicitation and applied scoring incentives for minority firms responding to this solicitation. If a Proposer is currently certified as an African American or Non-African American Firm, they would qualify to obtain the 10 available points as listed in Section 7.2.

Q115: For any exhibits that are not applicable (e.g., Exhibit 4 "Local Business Affidavit of Eligibility"), should our submission include a blank form? A form marked as "Not Applicable"? Or should we exclude the Exhibit from our submission?

A115: Any exhibits that are not applicable may be excluded from the submission.

Q116: Can you provide a network architecture diagram?

A116: Information will be shared as necessary once the solicitation is awarded.

Q117: How many network segments do you have? Physical Subnets and VLANS?

A117: Information will be shared as necessary once the solicitation is awarded.

Q118: How many firewalls in your network?

A118: Information will be shared as necessary once the solicitation is awarded.

Q119: How are you using the public cloud? Which one(s)?

A119: Information will be shared as necessary once the solicitation is awarded.

Q120: Do you have an existing Written Information Security Program?

A120: Information will be shared as necessary once the solicitation is awarded.

Q121: Do you currently have a Written Incident Response Plan?

A121: Yes

Q122: Does M-DCPS currently have an MDR solution?

A122: No

Q123: Do you believe you have been compromised?

A123: No

Q124: Is a 3rd party Managed Service Provider currently utilized by M-DCPS?

A124: No

Q125: Is a Digital Forensics process, technology or both desired?

A125: This request is for a process or service, but proposers are welcome to provide a separate line item for a technology solution if desired as a value-add.

Q126: Is M-DCPS responsible for Scan and Pen Tests results remediation?

A126: Yes

Q127: Is M-DCPS organized under a Central IT department or are there different IT departments?

A127: Yes, one central IT Dept.

Q128: How many staff members are dedicated to the Cyber and Information Security organization for M-DCPS?

A128: Less than 20 full-time employees.

Q129: Is there a dedicated CISO employed at M-DCPS? Who does the CISO report into?

A129: Yes; the CISO reports to the CIO.

Q130: Does M-DCPS have a formal asset management program? If so, would you please provide the following:

a. Number of network devices
b. Number of servers (physical and VM)
c. Size of wireless network (controllers, access points, etc.).
d. Number of total applications

A130: Information will be shared as necessary once the solicitation is awarded.

Q131: Please confirm we can use Sub-Contractors to meet some of your requirements.

A131: Subcontracting is permitted under this contract. The vendor shall be held fully responsible and liable for the supervision and performance of all work performed by subcontractors. M-DCPS shall not be responsible for resolution of disputes between the vendor and any subcontractor.

Q132: Can you provide an update on the award timeline for RFP 21-034-CM Network Security Assessment? Since the winner of that work will not be awarded RFP-21-009-VF, it would be useful to know whether we should expect an award decision before this newer response is due.

A132: At this time, the solicitation is still under evaluation and no company has been recommended or submitted for award.

Q133: Can you provide additional detail on your managed detection and response requirements? Are you looking for an MDR solution to be implemented? If yes, can you also answer the following questions?

- **How would you like pricing to be provided for an MDR solution? Pricing is dependent on number of locations and assets in scope, not hourly rates.**
- **How many locations and assets are in scope for an MDR solution?**
- **Are you open to cloud-based "as-a-service" solutions?**
- **Are you looking for 24x7x365 monitoring?**

A133: No, the District is not looking for an MDR.

Q134: Can you provide clarification on what is required for the "local business tax receipt" and "license" for businesses based outside of Miami-Dade County? IT consulting services are not a regulated business which require an occupational license.

A134: The Miami-Dade Local Business Tax Receipt confirms payment of the Local Business Tax. A business located within the municipality is required to obtain a County receipt. If your business is located outside of Miami-Dade County, provide a copy of your local municipalities' business tax requirement compliance. If your municipality does not require a business tax, please submit a statement confirming so.

Q135: Can you provide the number of IP addresses in scope in the internal and external networks for penetration testing?

A135: Information will be shared as necessary once the solicitation is awarded.

Q136: Can you provide the number of locations and SSIDs in scope for wireless testing?

A136: Information will be shared as necessary once the solicitation is awarded.