ADDENDUM NO. 3

September 4, 2020

RE: RFP 002.21.B5, Managed Security Services Solution

FROM: Purchasing Office
Howard County Public Schools
10910 Clarksville Pike
Ellicott City, MD 21042
(410) 313-5644

TO: PROSPECTIVE BIDDERS

This addendum modifies the Original Bidding Documents as noted below. Acknowledge receipt of this Addendum in your Proposal. Failure to do so may subject the Bidder to disqualification.

---

1. INSERT Questions & Answers

No.	Question	Answer
153.	Scope of Work 4.1.e. 1) Any specific geo-based data restriction? 2) Specific Threat database to be used or Partner database is ok? Any Specific Compliance followed by Customer?	1) Yes. See Section I in RFP Attachment C – Client Data Sharing Agreement. 2) Vendor recommends in response 3) FERPA, HIPAA, see #37
154.	Scope of Work 4.1.g. 1) How many firewalls are in this Scope? 2) Super-Admin Access is required Change management is there or Partner have full-privileges to make changes?	1) 2 2) Not a question Change management exists. No.
155.	Scope of Work 4.1.i. 1) Incident response on firewalls? Or for the whole network? If yes, is there any existing tools that client is using to monitor and incident management. Also, Is there any case management or any ticketing solution?	1) Yes, whole network, yes Yes
156.	Scope of Work 4.1.j. 1) What is the expectation with this SOW. Does the client just need scanning, or need scanning and patch management? 2) Also does the client need remediation? Vulnerability Scanning is required or Penetration is also included. (As penetration may involve service downtime)	1) Both 2) Yes Vulnerability management is required. Penetration testing is not.

No.	Question	Answer
157.	Scope of Work 4.1.1 Alternate 1 regarding Full Management, User Management, Administration and Maintenance for Palo Alto, Aruba & Cisco Nw devices and other SaaS applications 1) Super Admin privileges are required Number of final user in Scope to be handled"	1) Not a question See Answers #50, #66, and #139
158.	Scope of Work 4.1.4.1 Improved mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) for incidents. 1) Is the client referring to SLA? what is the existing MTTD and MTTR?	1) Yes Unknown
159.	Scope of Work 4.1.7, Fault Tolerance Please share me more details on this, as they require fine tuning of configuration on all devices	Seeking uptime and redundancy in respect to fault tolerance. See sample SLAs
160.	Scope of Work 4.1.10, Contractor On-prem or On cloud solution?	Solution can be either.
161.	Scope of Work 4.2.3, Permission to Proceed Required Physical as well as remote management permissions	The offeror would coordinate with HCPSS the location and layout of all equipment for each location prior to commencement of work. This applies if you must install devices on-premise. Remote management permissions would be coordinated with HCPSS.
162.	Scope of Work 4.2.4, Damage and Cleanup Restoration and data storage will be at Partner Data center, or customer has its own data storage servers	Yes
163.	Scope of Work 4.2.14, Database Entry 1) Average data flow (Gbps) monthly/quarterly/Yearly 2) Log Retention is required? Hot/Cold Storage is required"	1) Unknown 2) See Answer #137 3) See Answer #137
164.	Scope of Work 4.2.23.1, .2, .3, and .4 Service Level Credits Can the penalty clauses be relaxed?	No
165.	Scope of Work 4.2.26.1 Service and Support Partner for any on-premise related requirement.	Not a question
166.	Would the County please clarify what "technical criteria" means as referenced in Section 5, subsection 1.1 of the RFP?	Evaluation components by which Offerors will be scored
167.	How do the contents of Section 5, Subsection 3 of the RFP relate to the "technical criteria" referenced in Section 5, Subsection 1.1 of the RFP?	Tab 1 and Tab 2 responses will be evaluated respective to the technical criteria.
168.	To satisfy the HCPSS requirement for "monitoring and logging of network traffic..." (Scope of work 1.a), should the offerors bid full-time, full packet capture?	Full-time, full packet capture may be required for threat and risk management
169.	Please define "outages" as used in Scope of Work Section 2.26.3.3. Specifically, is HCPSS referring to critical outages in the contractor call center and SOC?	An outage would be disruption of service. Yes, and at HCPSS locations.
170.	Please explain the service levels described in Scope of Work Section 2.23.3 - Weekly Median Incident Resolution	It represents a cumulative penalty for not meeting SLA for consecutive weeks.

No.	Question	Answer
	Time SLA. Specifically, how are minutes related to weeks in your service levels?	
171.	Would the county consider extending the RFP response deadline based on the short period of time between answers to the second round of questions and the bid due date?	No
172.	What HCPSS have any problem with hosting cyber event data on AWS?	No, if it's fully managed and paid for by the offeror.
173.	Are there any data aggregators that control North/South traffic across the network?	No
174.	What type of ticketing system does the IT department use?	See Answer #127
175.	Confirm the total # of hosts/IPs in scope for vulnerability management.	500
176.	Do you expect the provider to include vuln management software/tool?	Yes
177.	Do you expect the vendor to provide remediation of identified vulnerabilities?	See Answer #82
178.	Would East/West monitoring be per site (school) and/or within the data centers?	See Answer #5
179.	Is Live data visualization an existing capability in existing security tooling or would a new solution to meet this requirement be required? If an existing capability, what's currently being used?	No, not required, Palo Alto, MRTG
180.	Is it HCPSS' objective to implement endpoint monitoring for all 68,461 endpoints?	Will be based on Risk
181.	If so, would HCPSS want Microsoft Defender ATP extended to all ~68,000 endpoints?	ATP is already installed on all Windows products
182.	Other than Microsoft Exchange ATP, are there any other spam protections in place?	No
183.	How many estimated number of endpoints are currently being ingested into SIEM?	0
184.	Do all sites send logs to SIEM?	No
185.	What types of logs are sent to SIEM?	N/A
186.	What is the current data storage capacity of the SIEM?	N/A
187.	Does the current SIEM infrastructure have enough data storage for all sites and systems within scope?	No
188.	Do any Palo Alto firewalls have SSL decryption enabled/in use?	No
189.	Are SLA based off of prequalified alerts and/or incidents or is an alert tuning period allowed?	An alert tuning period is allowed.
190.	Is the pervasive wireless in every site and school?	Yes
191.	Are Aruba ClearPass Network Access Control (NAC) capabilities fully implemented for both wired and wireless networks?	No
192.	Are monitoring of staff and student accounts & their devices in scope while any emergency (ie Covid-19	Yes. Staff and students are not required to use VPN.

No.	Question	Answer
	pandemic) remote teaching is in effect? As an example, are all staff and students required to use HCPSS VPN solution for active North/South monitoring and management?	
193.	In Addendum #2 of RFP #002.21.B5, the answer to question #7 indicates student activities, devices, and accounts are in scope of this RFP, but #94 states that student devices are not in the scope. Can you clarify under what circumstances student devices are covered in the scope of this RFP?	**REPLACE**: **Answer** to Question #95: "Are student devices within the scope of this RFP?" **with "Yes"**
194.	In addendum #2 of RFP #002.21.B5, the answer to Question #128 indicates there are an estimated 40 tickets per month. Are change requests the only tickets counted in this total? If not, what is the total estimated number of tickets?	No. Unknown.
195.	What's the total estimated number of priority 1 tickets per month?	Unknown
196.	The SLAs list an expected up-time for an SOC MSSP portal. Is there an existing MSSP portal or does that need to be created.	A customer-facing portal should be provided.
197.	Is the MSSP portal a mandatory requirement if not already in use?	A customer-facing portal to the solution is a requirement.
198.	Which Microsoft operating systems are in use in servers and/or endpoints. Which end-of-life/outdated operating systems are still in use (such as Windows 95/98/Vista)? Which versions of MacOS are in use?	No end-of-life products are on the network
199.	Which versions of Linux are in use?	Centos and Ubuntu
200.	What Anti Virus/Endpoint Detection & Response (AV/EDR) software is in use for non-Microsoft operating systems?	Microsoft Defender ATP
201.	What is the current EPS (Events per second)?	Unknown
202.	Can the SOC services be provided from an offshore certified facility?	No
203.	Is there a local syslog server available?	No
204.	What is the access management solution currently used to manage the user's access to SaaS applications like Workday, Synergy, Canvas, Hoonuit?	Custom scripts
205.	Is there a specific regulatory / legal requirement to be addressed/ adhered to?	See Answer # 37
206.	Are student devices included in the scope of this RFP?	Yes

END OF ADDENDUM