



**ADDENDUM NO. 2**

**August 28, 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
1.	Are there any small business requirements for this project?	No
2.	For the Staff Augmentation Option, how many hours per week or per month do you anticipate needing for Palo Alto, Aruba, Cisco, Microsoft365, Gsuite, Workday, Synergy, Canvas & Hoonuit?	Unknown
3.	Will HCPSS consider awarding Managed Security roles/responsibilities separate from the SaaS applications end-user management?	Yes
4.	Is the priority outsourcing the administration and maintenance or managed detection & response?	Both
5.	Describe the East/West monitoring you'd like and the network locations where we could monitor that traffic (router/SD WAN/concentrator)	Understanding lateral network movement when investigating an incident is helpful. Traffic between critical systems located in both data centers would be a target when investigating. The layer 2/3 gear would be a likely source to use for monitoring.
6.	Please list the cloud and any other key systems you expect to integrate into the MDR platform	Azure, AWS, M365, G-Suite for Education, Workday, Canvas, Hoonuit, Digital Ocean, perimeter protection gear, VPN concentrator, routers, switches, Active Directory, backup systems
7.	Are student accounts, devices, and activities in scope for monitoring? If not, please describe how the students are segregated from the network otherwise – separate SSID/VLAN/Active Directory/Internet connections/etc	Yes. We use separate VLAN and AD Domains.

No.	Question	Answer
8.	Please define vulnerability management – what capabilities are you looking for? Identification, prioritization, remediation, etc?	The cycle includes identify, classify, prioritize, remediate, and mitigate.
9.	Are you willing to separate application management and threat detection? Specifically, would you award the bid to one vendor that can provide threat detection and response to O365, G-Suite, Workday, Synergy, Canvas, and Hoonuit but not user management?	HCPSS reserves the right to make a one award, multiple awards, a partial award, or no award at all.
10.	Does the school system have a SIEM today? If so, which SIEM? If not, do you have a preferred SIEM that is commercially available?	No to both.
11.	Are there use cases outside of threat detection and response that are required?	HCPSS is looking for a vendor to help with that question.
12.	Does the school system have EDR on the endpoint today? If not, do you have a preferred endpoint. For example, you have Palo Alto Network firewalls. Do you prefer CORTEX XDR or another tool?	No preference if fully managed by respondent.
13.	Is this for one solution or an RFP to obtain multiple?	Either - For a solution(s) that ( <i>cumulatively</i> ) meets the needs of HCPSS as set forth in the RFP
14.	Is the primary goal to acquire MDR services (section 1) and Alternates 1 & 2 are additional/optional components?	Primary is MDR. Alternate 1 and Alternate 2 are optional, as HCPSS may entertain.
15.	Do we have to choose to respond to either Alternate 1 or Alternate 2? Or can we respond with a hybrid solution that includes portions of each option?	You do not have to respond to Alternate 1 or Alternate 2. If your response to MDR includes elements of the alternates, HCPSS would want to see pricing broken out as noted in the pricing section.
16.	Is the onsite Project Manager a true requirement? In light of COVID, most Project Management services are being delivered/managed remotely.	Considering the Covid pandemic, the project management can happen remotely
17.	If the onsite Project Manager is a true requirement, can you please explain why they are required to be onsite?	Considering the Covid pandemic, the project management can happen remotely
18.	Are service level credits a hard requirement? Or a negotiable item?	Negotiable
19.	Will you consider extending the due date?	See paragraph 1 above in this addendum for revised due date
20.	Will HCPSS please confirm what G Suite services are enabled in the domain (e.g., Gmail & Messaging, Chat & Hangouts / Meet, Drive & Collaboration, Classroom, Vault for EDU, etc.)?	Google For Education – No Gmail, Classroom or Vault
21.	Is HCPSS open to a multiple award schedule where multiple vendors provide Alt. I and Alt II services for specific solutions?	All proposals will be accepted. HCPSS may make one award, multiple awards, or no award at all. The goal is to contract with a company(ies) that best meets the needs of HCPSS as set forth in the RFP. See paragraph 1.9, Rejection or Acceptance of Proposals.

No.	Question	Answer
22.	Will HCPSS please provide additional insight into MDR services versus Alternate 1 or Alternate 2 services?	Primarily, HCPSS is seeking MDR services. If your organization can offer specific managed services for systems listed in Table 1, provide information and pricing. This will provide the opportunity for HCPSS to consider specific managed services outside of the MDR offering. If your organization can offer engineering at an hourly rate on an ad-hoc basis for system listed in Table 2, provide information and pricing.
23.	Will HCPSS please confirm what edition of G Suite for Education is being used (e.g., free edition for EDU or G Suite Enterprise for Education)?	Currently using G Suite for Education – Evaluating G Suite Enterprise for Education,
24.	Will HCPSS please confirm if Google Chrome and Chromebook device management is in scope for this RFP?	Yes
25.	Will HCPSS confirm that delivery of staff augmentation for G Suite managed services can be performed remotely?	Yes
26.	Under Project Scope, item g references firewall management. Is this scope item specific to incident response?	Yes. The MDR section is inclusive of incident response and would require firewall management as part of the MDR service scope. Alternate 1 provides a listing in Table1 of systems that are candidates for traditional managed services, not MDR.
27.	This RFP seems to be specific to managed detection and response, as described under Project Scope. Can HCPSS please elaborate as to how Alternate 1 or Alternate 2 ties to overall project scope?	Primarily, HCPSS is seeking MDR services. If your organization has the ability to offer specific managed services for systems listed in Table 1, feel free to provide information and pricing. This will provide the opportunity for HCPSS to consider specific managed services outside of the MDR offering. If your organization has the ability to offer engineering at an hourly rate on an ad-hoc basis for system listed in Table 2, feel free to provide information and pricing.
28.	The RFP does not appear to contain relevant data that fully describes the IT processing environment in scope to assist in pricing. Is HCPSS amenable to completing a scoping questionnaire? If that is not possible, at this time, can you HCPSS please provide a breakdown of security technologies, servers, and other relevant infrastructure that in scope for log ingestion and log analysis?	No. No.
29.	HCPSS has included termination for convenience language within the Special Terms and Conditions of the contract. Is this clause a "hard" requirement or should we price this convenience factor into the overall proposal?	Paragraph 3.13, Termination For Convenience, cannot be removed
30.	For ease of RFP response, would it be possible to receive this document in original form, prior to being converted to .pdf?	No

No.	Question	Answer
31.	The timeline between responses to these questions and RFP submittal is quite tight. Would it be possible to modify the Bid Due date to September 8th?	See paragraph 1 above in this addendum for revised due date
32.	What is the average amount of monthly incidents over the past year?	10
33.	Additionally, current monthly average of resource time consumption (over 1-year sample)	20
34.	Is MSSP required to utilize (alert/report) client incident tracking platform?	No
35.	Is there a pre-defined list of expected threat, alert types, and thresholds for devices or will MSSP determine the alert and response lists? Ex. specific windows security event logs, etc.	No
36.	Is the SIEM platform allowed to perform scheduled and OnDemand vulnerability assessments?	Yes
37.	What regulatory frameworks and controls is the client obligated/adopted to follow as it relates to cybersecurity?	MD DoIT Security Policy as interpreted by the MD Office of Legislative Audits
38.	Are all systems in Table 1 & Table 2 maintained under current manufacturer warranty, licensing, IOS updates, and security patching?	Yes
39.	Are there specific SIEM reporting requirements such as frameworks, types, data fields, trending, or other report needs beyond just incident response/mitigation reports?	Reports that support SLA agreements. Other example reports would be top attackers, top attacked hosts, top used ports, top alarms, top events by risk, asset detail reports, etc. No specific frameworks have been adopted.
40.	Is there any special physical (or logical) network segmentation that may require separate event collector appliances, i.e., IT vs OT networks?	Yes
41.	How are HCPSS networks connected, routing, security, and available bandwidth?	Fiber, 1GB Elementary Schools, 3GB Middle schools, 5GB High schools, 10GB Internet
42.	Can there be a centralized event collector serving all datacenters or will each datacenter require a dedicated event collector?	Yes
43.	Is there a published SLA response requirements/expectation for L1-3 services?	A published SLA is not published internally. Sections 2.23 and 2.26 provides some guidance on expectations for SLAs. Offerors may provide their standard SLA for HCPSS' review.
44.	Where does your infrastructure reside in? Your data center, a public cloud, a virtualized private cloud, or a combination?	Two Data Centers within the county. We have limited use of AWS and Azure.
45.	What do you use today to detect cyber threats that have breached or are attempting to breach your organization?	Microsoft E5 and Palo Alto technologies.
46.	If you have a cloud infrastructure, how is it secured today?	VPN to Azure
47.	How many Servers do you have within your Environment?	461
48.	How many Firewalls do you have within your Environment? Are they all the same make & model?	2, yes

No.	Question	Answer
49.	How many total devices would the contractor be responsible to monitor/manage?	See Question 50 Firewalls-2, Routers – 81, Switches - 1625
50.	What is the quantity/device break down on those devices (IE 20 Switches, 5 Routers, 2 Load Balancers, 100 Servers, 500 Workstations, 10 Firewalls, 5 SANs, Etc.)?	See Question 50  2 datacenters 2 firewalls 81 routers 1625 switches 20 cloud-based systems 461 servers 68,000 client computers
51.	What internal management tools does HCPSS utilize within the environment to manage the infrastructure today?	Microsoft and vendor specific management tools
52.	Will these tools still be utilized by the contractor or is the contractor expected to bring in its own infrastructure management tool set?	Existing tools could be used by the contractor. Additional tools recommended by the provider should be included in the cost.
53.	How may AWS Accounts or VPCs does the organization want to monitor?	4
54.	How many Azure resource groups does the organization want to monitor?	Less than 10
55.	Do you have a list of business processes or data ranked and based on importance to the school district? That is one of the first things we look at as a company in these situations. This could also be a business processes diagram of your infrastructure.	Yes
56.	<p>Page 4, Paragraph 18, Forms: “This entire solicitation document, along with any attachments indicated with the responses filled in, is to be submitted as the main part of the Offeror’s proposal.” This statement seems to conflict with the information in Section 5. Some of the forms that are in the solicitation document don’t allow for vendors to do what is being asked.</p> <p>Attachment G is an example: Per Instructions in paragraph 4.7 on page 25, vendor must acknowledge compliance with HCPSS Contractor Performance/Evaluation Scorecard; however, within the solicitation document, there is no fillable field to use for making this acknowledgement.</p> <p>The same is true for Attachment B, and the checklist on page 28 is not fillable. It is presumed that HCPSS does not intend for vendors to return the solicitation document as the main part of the Offeror’s proposal; instead, HCPSS intends for vendors to follow the instructions in Section 5,</p>	<p><b>DELETE</b> the following sentence on Page 4, Paragraph 18, Forms:  <u>“This entire solicitation document, along with any attachments indicated with the responses filled in, is to be submitted as the main part of the Offeror’s proposal.”</u></p> <p>Acknowledgment of Scorecard is on the <u>Attachments and Forms (Check List)</u></p> <p>Attached is a fillable <u>Attachments and Forms (Check List)</u> form</p>

No.	Question	Answer
	and make necessary adjustments without changing any of HCPSS' solicitation language – is this correct?	
57.	Does HCPSS, the State of Maryland, or another agency in Maryland currently have a contract with a managed security services provider? This question is based on page 8, paragraph 13, Multi-Agency Participation.	Unknown
58.	Page 23, paragraph 2.27: Is the review annual (once per year) or bi-annual (twice per year)? Currently the paragraph seems to indicate both.	Annually
59.	Page 24, item 3.5, Five-Year Support: "Provide letters from both the Offeror which guarantee the solutions will be supported for a minimum of five years from the installation cutover date." – Only the Offeror is listed; it is presumed that "Subcontractors" was meant to be included; hence the use of "both". Please confirm.	As the Contractor is responsible for all sub-contractors <b>CHANGE</b> this sentence to: <u>"Offeror shall provide a letter which guarantees the Solution will be supported for a minimum of five years from the installation cutover date."</u>
60.	Please clarify whether Attachments K and L (Pricing Questions and Cost Worksheet, respectively) are supposed to be included in the Technical Proposal or the Pricing Proposal. Per the bottom of Page 25 (Section 5, SUBMITTAL REQUIREMENTS AND PROPOSAL FORMAT), it looks like Attachments K and L are supposed to be included in the Technical Proposal (Sections 3 and 4 on pages 24 and 25 indicate what to include in the Technical Proposal, correct?) and Page 27, SECTION VI. PRICE PROPOSAL indicates what should be in the Price Proposal. The information on Page 27 appears to conflict with the information on pages 24 and 25 (24 and 25 seem to indicate that both Attachments K and L should go in the Price Proposal along with a Bill of Material and value-added services).	Only Attachment K shall be submitted with the Technical Offer.  Only Attachment L shall be submitted with the Price Proposal.
61.	Please confirm that vendors do not need to complete any part of Attachment F for proposal submission.	Correct. An Offeror shall acknowledge acceptance in the <u>Check List</u> that agree to utilize the HCPSS Agreement template.
62.	In Attachment D, the "TECHNICAL PROPOSAL DUE DATE:" field doesn't have a fillable form field next to it; thus, no way to add the due date. Will an updated form be issued for completion, or shall vendors ignore this field?	An updated page <b>is attached</b> .
63.	Page 28, Attachments and Forms (Check List): Where in the technical proposal should this checklist be located - e.g., before or after the transmittal letter, or as the last item?	Insert Attachments in alphabetical order.
64.	Technical Proposal Questions Project:	
65.	a) How many systems under management?"	68,000
66.	b) How many users?	11424 staff, 58352 students
67.	c) How many local systems? (Desktops, Servers)	68,000
68.	d) How many cloud-based systems?	20

No.	Question	Answer
69.	e) Are cloud-based systems under management by external vendor?	0
70.	f) How many hosted systems?	68,000
71.	g) Where are systems hosted?	HCPSS 80 locations
72.	h) What are the current patch management systems?	G Suite, WSUS, SCCM, Intune
73.	i) What are the current monitoring tools and software in use?	Xymon, Dell OpenManage
74.	j) How many internal users?	11424 staff, 58352 students
75.	k) How many external users?	11424 staff, 58352 students
76.	Is a network diagram available?	See attached <u>Systems Architecture Diagram</u>
77.	Will the network design be hub and spoke or mesh? Or will this be a hybrid?	Hub and Spoke
78.	Will there be a primary and secondary WAN connection to each site, and what type of connections are there? (MPLS, broadband, LTE, etc)?	No, Single connection to each site using county fiber network.
79.	What are the bandwidth requirements per site?	1GB ES 3GB MS 5GB HS 10GB Data Centers
80.	Is on-site support required for the solution implemented?	No
81.	End Point Protections <ul style="list-style-type: none"> <li>How is end point protection addressed by HCPSS? Please confirm that end point management is not included in the RFP.</li> </ul>	Microsoft Defender ATP. Vulnerability management would be part of the MDR solution.
82.	Section 4 – Scope of Work 1. Project Scope i. Incident response and remediation by third-party provider. <ul style="list-style-type: none"> <li>What are the responsibilities of the Managed Security Service Provider with Incident response and remediation since it references a “3rd party provider”?</li> </ul>	The offeror is the “third party provider” to HCPSS. The incident response cycle would include detect, analyze, contain, recover/remediate, post-incident analysis. Remediation would involve working with system owners and/or being provided the access to perform the incident response activities required.
83.	Section 4 – Scope of Work 1.1 Alternate 1. Managed Services for Systems. “HCPSS will consider third-party management of selected devices, platforms, services, or applications to ensure ongoing security in operation and administration.” <ul style="list-style-type: none"> <li>For the Table 1 systems in 1.1, is full management only related to security monitoring or does it include full operational responsibility like device monitoring for availability, performance, uptime, etc.? Also, will the contractor monitor and manage</li> </ul>	Full management would not only include security monitoring but full operational responsibilities such as device monitoring for availability, performance, uptime, etc. Firewall management is noted as a requirement for the MDR. Service requests for LAN/WAN will be handled internally.

No.	Question	Answer
	all firewall and LAN/WAN device related service requests?	
84.	<p>Section 4 – Scope of Work</p> <p>1. Project Scope</p> <p>1.2. Alternate 2. Staff Augmentation. “HCPSS will consider third-party staff augmentation used on an ad hoc basis for systems listed in the table below.”</p> <p>Table 2</p> <ul style="list-style-type: none"> <li>• Will HCPSS select multiple vendors for the systems management in table 2?</li> </ul>	HCPSS reserves the right to make a one award, multiple awards, a partial award, or no award at all.
85.	<p>Section 4 – Scope of Work</p> <p>1.4.3. Proactive threat hunting and reporting that includes endpoint identities and user identities, where possible.</p> <ul style="list-style-type: none"> <li>• Does the contractor create a bucket of hours for Threat Hunting with a T&amp;M rate for more time if desired by HCPSS?</li> </ul>	HCPSS would want proactive threat hunting to be a standard part of the MDR service.
86.	<p>Section 4 Scope of Work</p> <p>1.11. Serviceability: Contractor shall be responsible for all system maintenance, upgrades and hardware replacement for Solution provided.</p> <ul style="list-style-type: none"> <li>• What is the life of the equipment under management?</li> </ul>	All equipment under management have a maintenance support agreement.
87.	<p>Attachment B – Insurance Requirements</p> <p>Section 2.1.5</p> <p>Will HCPSS consider striking the Aircraft Liability requirement?</p>	Yes
88.	<p>Attachment B – Insurance Requirements Section 4 – Builders Risk Insurance</p> <ul style="list-style-type: none"> <li>• Will HCPSS consider striking the Builders Risk Insurance requirement?</li> </ul>	Yes
89.	<p>Table 1</p> <p>Tasks to Outsource - Applications</p> <ul style="list-style-type: none"> <li>• What is the scope of the management of the applications listed in Table 1? The “Tasks to Outsource” column in Table 1 suggests that the contractor will be responsible for managing the applications listed.</li> </ul>	Administration and maintenance include but is not limited to various log reviews, backup verification, track/monitor system performance, check hard disk space, user/account administration, antivirus event reviews, firmware/software updates, operating system updates, application updates, troubleshooting, and reporting.
90.	The submittal requirements listed in section 5 (pages 24 and 2 separate the attachments from the overview by "Tabs." What exactly is meant by "Tabs?"	A Tab is a sub-section
91.	Section 2 of the Scope of Work requires that "personnel listed in the Respondent’s proposal shall be the personnel assigned to this project." In the immediately subsequent section, the government defines responsibilities of the	Yes. See paragraph 3.5, Professional Services.



No.	Question	Answer
	contractor Project Manager. Is it the government's expectation that the contractor Project Manager be listed by name (a.k.a., be bid as key personnel) in our proposal?	
92.	What types of devices are included in HCPSS' existing infrastructure under "Endpoint totals?"	See question 50.
93.	Given your list of Desktop Software does not include mobile technologies (e.g., Chromebooks, tablets, mobile phones), should we assume mobile technologies are out-of-scope for this RFP?	No
94.	Are student devices within the scope of this RFP?	No
95.	How many, and which, data sources are currently monitored by Microsoft Sentinel?	All services included in Microsoft E5
96.	How do you define "Incident" as used in section 2.23 of the Scope of Work?	A security incident is an event that is a viable risk or that causes damage such as lost data or operational disruptions.
97.	Can you please provide the quantities and model #s for Palo Alto FWs? Also, indicate if single or HA pair.	Palo Alto 5280. One in each Data Center, they are standalone.
98.	How many domain controllers are in scope?	4
99.	Are all 120,000 endpoints covered with either Windows ATP or Wildfire?	No
100.	Can you confirm the number of O365 accounts in scope?	8,500 staff 58,700 students
101.	Can you specify the OS for the 450 servers? Windows? Linux?	Windows 2012 and 2016. ~5% Linux
102.	You requested that we identify resources who would support this project. We have a broad team of resources that could support this RFP. We wouldn't be able to identify the final resources until the project has been awarded and we are ready to begin work. Can we provide sample resumes of some of our resources that could possibly support this project instead?	Yes. HCPSS seeks to understand the roles/expertise for supporting the proposed solution.
103.	Scope of Work: If additional tools are required or recommended by us / approved by HCPSS would they be procured / licensed or subscribed by HCPSS or would the Contractor be required to provide them?	See question 52
104.	Scope of Work: In case of 1 above ( <i>question #103</i> ) – a) who would be negotiating for support agreements with suppliers? b) Would the Contractor be responsible for ensuring support over the contract term?	a) Assignment to dept. or staff member(s) would depend on numerous factors b) Not enough information to provide answer
105.	Scope of Work: Who is the incumbent vendor? For Managed Services and/or Staff Augmentation?	N/A
106.	Scope of Work: How is Security currently being managed? By HCPSS or Contractor?	HCPSS

No.	Question	Answer
107.	Scope of Work: There are 2 Alternatives. Is the Contractor expected to provide a response to both or any one of them?	Either or both
108.	Will it be acceptable if we provide only MDR service and not the "Managed Services for Systems" which is 1.1 alternate 1 and 1.2 alternate 2?	Yes
109.	Please provide the total number of security devices (Layer 3 and above) (E.G. NextGen FW, simple FW, standalone IDS/IPS, etc.) to be monitored:	Palo Alto 5280. One in each Data Center, they are standalone.
110.	Do you have an EDR? If yes, how many endpoints are on it?	Microsoft Defender ATP, 12,000
111.	Do you have an AV/EPP? If yes, how many endpoints are on it?	Microsoft Defender ATP, 12,000
112.	Please list the no. of L3 Switches & Routers that needs Log monitoring	Aruba 2930M – 1350 Aruba 3810M – 200 Aruba S3500 – 75 Cisco 3560 – 33 Juniper SRX – 44 Cisco 4500 – 4 Cisco 6509 – 2 Cisco 3850 - 22
113.	Please list the no. of On-Prem Servers and Databases to be monitored	461
114.	Please list the no. of O356 Users	8,500 staff 58,700 students
115.	If you want to add any of the user source like AD/ Email gateway/ VPN, please let us know the number of users for each of the sources	AD and Email: 8,500 staff 58,700 students. VPN: ~200 staff
116.	Please list your cloud workloads (Instances, Storage, DB) and its count- AWS_____ & Azure_____	Azure virtual machine, 9 Azure VPN gateway, 1 Azure storage account, 13 Azure front door, 2 Azure cosmosdb, 1 Azure function app, 1 Digital Ocean, 6 droplets powering 85+ sites Digital Ocean, 6 Elastic IPs AWS S3, 8 buckets AWS Route 53, 7 hosted zones AWS Elasticsearch Service, 1 domain and 80 indices AWS SES, 1
117.	Do you have any other SaaS application (example: Salesforce, Okta) that you wanted include under monitoring?	See Question 6
118.	Please list if you have any cloud security resources in AWS or Azure(FW/ WAF/ AWS GuardDuty, Azure Sentinel)	Everything included in Microsoft E5
119.	Approximate volume of Flows (VPC flow logs/ NSG flow logs, in GB/ day) in AWS or Azure	Unknown

No.	Question	Answer
120.	What is the scope of the IT environment we will be monitoring 24x7x365? Can you supply the breakout per endpoint? What are the number of endpoints and servers in scope for this RFP?	See Question 50
121.	Number of endpoints (laptops, desktops, servers),	461 servers 68,000 client computers
122.	Number of network devices (firewalls, routers, switches),	Firewalls-2, Routers – 81, Switches - 1625
123.	Main/Key cloud applications (O365 etc.)	O365
124.	Number of users within the County (O365 or Exchange users, Active Directory users)	8,500 staff 58,700 students
125.	Does the County own a SIEM license currently? If so, which product and when does the license expire.	Microsoft Sentinel, July 2021
126.	Does the County own an Endpoint Detection and Response Solution license currently? If yes, how many endpoints are on it?	Microsoft Defender ATP, 12,000
127.	What Ticketing platform/system is used by the County today? Any plans to change in the next 3 years?	Webhelpdesk and the Hive, no
128.	Estimated total tickets by weekday (8am-5pm)? Estimated total tickets by nights/weekends? % of tickets that are a P1? Estimated change requests in a week/month?	40 change requests/month
129.	Is there a current SOC Service vendor? If so, can you provide information related to their services?	No
130.	Are standards like SOC2 Type2, ISO27001, Privacy Shield or GDPR (or similar) required by the county? Will additional consideration be given to providers that hold these compliance-based certifications?	The certifications are not a requirement but are preferred.
131.	How many physical sites will be monitored as part of this scope? (Office locations, cloud environment, datacenter etc.)	82
132.	How many total locations (ingress/egress)? Please explain Internet connectivity for each location.	82. Each site connected via the HoCo fiber ring to the two data centers. Each Data Center connected to Internet (Cogent)
133.	Is the county looking for complete Incident Response (IR) included or more of a retainer to use per request?	Incident response should be included.
134.	Please provide the total number of security devices (Layer 3 and above) (E.G. NextGen FW, simple FW, standalone IDS/IPS, etc.) that need to be monitored.	Palo Alto 5280. One in each Data Center, they are standalone.
135.	Is there expectation of any having any other SaaS application (example: Office365, Salesforce, Okta) that you wanted include under monitoring? If so, we would need scope and size of those applications as well.	Not at this time. Refer to the provided Tables in the RFP.
136.	Approximate volume of NetFlows (VPC flow logs/ NSG flow logs, in GB/ day) in AWS or Azure?	Unknown
137.	What is your requirement for log retention? What is the expectation for HOT/COLD log retention – Compliance section says 365 days but how many days should be readily available? [Typically, we recommend 90days hot and rest COLD]	90 days available in 10 minutes 365 days available within 24 hours

No.	Question	Answer
138.	What total number of users are in scope for this RFP?	8,500 staff and 58,700 students
139.	Should we assume 8,500 users per application? If no, please list the no. of Users per application: <ul style="list-style-type: none"> <li>• MS365</li> <li>• G Suite for Education</li> <li>• Workday</li> <li>• Synergy</li> <li>• Canvas</li> <li>• Hoonuit</li> </ul>	<ul style="list-style-type: none"> <li>• M365 - 67200</li> <li>• G Suite for Education - 67200</li> <li>• Workday - 8500</li> <li>• Synergy - 97200</li> <li>• Canvas - 97200</li> <li>• Hoonuit - 8500</li> </ul>
140.	Is True North Consulting Group precluded from responding to this RFP as Prime contractor or Sub-contractor?	Yes
141.	Is the submission of representative resumes required?	Yes
142.	Has Howard County Public Schools previously had a Managed Security Services Provider?	No
143.	Is there an incumbent contractor providing similar services to those outlined in the RFP?	No
144.	Are the software/hardware products listed in Alternate 1 and Alternate 2 to be purchased by the Managed Security Services awardee?	No. These systems exist and are in production. The awardee would be provided necessary access to the systems to perform required work.
145.	Who was the offeror providing existing software/hardware products listed in Alternate 1 and Alternate 2 -- for Managed Security?	There is no existing managed security provider for any of the items listed in the tables. HCPSS holds vendor support contracts through the manufacturers for each system listed.
146.	Do prospective offerors need to describe their facilities?	Yes
147.	Are there facilities requirements?	Information regarding HCPSS facility requirements are noted in the RFP. The verbiage discusses access and standards for installations if the provided solution requires physical placement of gear onsite.
148.	It doesn't appear that there is a Minority Business Enterprise (MBE) requirement. Is there an MBE goal?	No
149.	Is this the first time for this RFP from HCPSS or is there an incumbent for this project?	First time. No incumbent.
150.	Can you share the list of participants that attended the pre-bid?	Attached
151.	Would you be able to let me know what is Patrick Johnson's (True North) role in the project? Will they be responding to the RFP?	Consultant. No.
152.	Is there someone in IT or can you please send the Systems architecture diagram related to the RFP?	Attached

**Addendum #2 Attachment**

Request for Proposal No. 002.21.B5, Managed Security Services Solution  
Fillable Attachments and Forms (Check List)

**Attachments and Forms (Check List)**

		Offeror Recognizes/ Acknowledges Acceptance		
		Yes	No	
Attachment A	Signature Sheet ( <i>signature required</i> )	Yes	No	
Attachment B	Insurance Requirements	Yes	No	
Attachment C	Client Data Sharing Agreement ( <i>signature required</i> )	Yes	No	
Attachment D	Acknowledgement of Receipt of Addenda ( <i>signature required</i> )	Yes	No	
Attachment E	Bid/Proposal Affidavit ( <i>signature required</i> )	Yes	No	
Attachment F	Agreement for Professional Services	Yes	No	
Attachment G	Contractor Performance/Evaluation Scorecard	Yes	No	
Attachment H	Technical Overview	Yes	No	
Attachment I	Contractor, Process, Staff and References	Yes	No	
Attachment J	Exceptions and Clarifications	Yes	No	
Attachment K	Pricing Questions	Yes	No	
Attachment L	Cost Worksheet	Yes	No	

\* Submit this completed Check List with Technical Proposal

**Addendum #2 Attachment**

Request for Proposal No. 002.21.B5, Managed Security Services Solution  
Fillable TECHNICAL PROPOSAL DUE DATE

**Attachment D**

**ACKNOWLEDGEMENT OF RECEIPT OF ADDENDA FORM**

**RFP NO.:** \_\_\_\_\_

**TECHNICAL PROPOSAL DUE DATE:**

**RFP FOR:** \_\_\_\_\_

**NAME OF OFFEROR:    **ACKNOWLEDGEMENT OF RECEIPT OF ADDENDA****

The undersigned hereby acknowledges the receipt of the following addenda:

Addendum No. \_\_\_\_\_                                      dated \_\_\_\_\_

Addendum No. \_\_\_\_\_                                      dated \_\_\_\_\_

Addendum No. \_\_\_\_\_                                      dated \_\_\_\_\_

Addendum No. \_\_\_\_\_                                      dated \_\_\_\_\_

As stated in the RFP documents, this form is included in our Technical Proposal.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

## Addendum #2 Attachment

Request for Proposal No. 002.21.B5, Managed Security Services Solution

### Pre-Bid Sign Up

---

#### Company

- 1 22nd Century Technologies, Inc
- 2 AlxTel, Inc.
- 3 Applied Technology Services
- 4 BreakPoint Labs
- 5 CDW-G
- 6 Cira Infotech
- 7 CloudCover
- 8 Cradle Systems, LLC
- 9 CyberESI Consulting Group, Inc.
- 10 Cybergrid Solutions, LLC
- 11 Data Networks
- 12 DATASHIELD
- 13 DMP Technologies LLC
- 14 ECS Federal, LLC
- 16 Elite Strategy Global, Inc.
- 17 Engler IT
- 18 FireEye
- 19 Fiserv
- 20 GAVS Technologies N.A.
- 21 GCOM Software
- 23 IBM Security Services
- 24 InfiNetix, Inc.
- 25 Infosight
- 26 IPKeys Power Partners
- 27 Kitamba
- 28 Managed Methods
- 29 MGT-Consulting
- 30 NALAComm
- 31 Network Intelligence, LLC.
- 32 NII
- 33 Optiv
- 34 Paladion
- 35 Raytheon Technologies
- 36 Red River
- 37 Reston Consulting Group aka RCG, Inc
- 38 Securance LLC
- 39 Skyline Technology Solutions LLC
- 40 SysDataLogics Corp
- 41 T12 Technologies, LLC
- 42 TechnoGen, Inc.
- 43 vTech Solution Inc.

# Addendum #2 Attachment

Request for Proposal No. 002.21.B5, Managed Security Services Solution

## Systems Architecture Diagram

