ADDENDUM # 01

Date: October 10, 2022
Reference: Cybersecurity and Network Engineering Services

IFB Number: 2023TECH-92622

Effective this date, this addendum forms part of the contract documents and modifies the original RFQ. This Addendum shall be attached to and form a part of the plans and specifications. All bidders must acknowledge receipt of this addendum on the Bid Form.

Answers to Questions:

- Do you use both Aruba switches and wireless? YES
- If Aruba wireless, do you control the wireless with local Mobility Controllers? Instant.
- You say that you use AirWave. Do you intend to move to Aruba Central as a replacement management platform? Yes
- Do you still use some Hewlett-Packard IMC as a legacy management tool? ClearPass and AirWave
- What type of firewall(s) do you use? (Or confirm your continued use of CheckPoint). Do you intend to upgrade or change your firewall soon? SonicWALL NSSP
- Confirm that you do use Active Directory. If you do, how many current Active Directory accounts do you have? Currently use AD
- Is any of this work designed to be E-Rate-funded? No
- How many people in your IT department? 12
- Do you intend to add more IT people in the coming year or so? Yes
- What type of antivirus software do you use? Carbon Black
- Do you currently have a SIEM? No
- How many devices and applications do you plan to collect enterprise logs from? ~160
- Do you currently use Paessler Network Monitor? No
- Do you currently use the Dell Managed Detection and Response service now, or are planning to get it? Currently in use

- How many Valcom overhead paging/bell systems do you have now? One for each of your ten schools? Yes but controlled by a single pair of HA units

- Can we have a current network diagram? Not at this time

- How many devices (servers, workstations, wireless access points, switches, routers) would fall under our scope of responsibility? Can you provide a list or breakdown of make and model for the hardware? 851.
    - 577+ APs
      115 switches. The core at each location is also the “Router” (11 of the 115)
      2 Firewalls in HA
      18 physical VM servers
      110 +/- VM servers
      1 physical print servers – all others are virtual
      4-5 +/- Phone servers
      23 + camera servers
- Is all hardware covered under current manufacturer warranty or support? If not, are patches and firmware upgrades available outside of the warranty or support?
    - Not all hardware is covered. A lot of it is.
- Does the district use Microsoft Active Directory (or similar directory service)? Are all users and computers covered under that directory?
    - Yes. AD is in use for all staff and computers.
- Could you provide a recent network map?
    - Not at this time.
- Would our scope include patch management for servers, network devices, and workstations?
    - Not at this time.
- If responsible for patch management on *servers*, does that cover only the operating system or applications as well?
    - N/A
- If responsible for patch management on *workstations*, does that cover only the operating system or applications as well?
    - N/A
- In our role of monitoring, we will receive many alerts, some of which will require action. Who is responsible for taking such action? In-house IT or EIS? If our role is to pass along the alert information, to whom would we send it (e.g., a help desk, internal network engineer, etc.)?
    - In-house IT will receive alerts. RFP is to set up alerting.
- What portion of the district's IT infrastructure is in the cloud? What is the cloud service, and would we be responsible for monitoring that as well?
    - We have a decent amount in the cloud. Google Workspace will be the only cloud software monitored at this time.
- What are your hours of operation? Would we be expected to forward alerts or take actions outside of your hours of operations?
    - N/A
- How do you handle backup, and would we be responsible for monitoring backup processes?
    - Barracuda,yes

- When would the contract start and when would you expect monitoring to be fully up to speed?

    - ASAP, within 3-6 months.
- When was the most recent security audit? Could we see the resulting report?
    - October 2021, not at this time.
- Does the district require a full System Information and Event Management platform (SIEM) or is a syslog server sufficient?
    - syslog server
- For the security awareness training, what would be our role in managing it?
    - provide software, our team will set up and monitor.