Accelerate Progress for Students

Rennette R. Apodaca, MPA, CPPO
Executive Director

Scott Elder
Superintendent

DATE: 6/7/2022
RFP NUMBER: 22-057 NMM
RFP TITLE: Managed Detection and Response (MDR) Solution
ADDENDUM NUMBER: 1

See Question and Answers

Question: Does the product/solution proposed by the vendor need to be covered under that vendors State contract vehicle? Or will this RFP serve as the purchasing contract for the product/solution?
Response: This is a separate RFP and will serve as the purchasing contract. It's not a state contract.

Question: What is the total number of Windows, Linux, MacOS machines in the environment? (Laptops, Desktops, Servers (physical or virtual), VDI sessions, etc.?
Response:
Windows: 11,000

MacOS: 9,000

Servers: 0 servers to be covered.

Question: How many Windows 7, Windows Server 2008, and MacOS X machines? Please identify 32 bit or 64 bits
Response:

Windows 7 64-Bit: 120

Windows 7 32-Bit: 40

Windows Server 2008: 0

Windows Server 2008 R2: There are 75

MacOS: 9,000

Question: How many total data centers? Primary/Backup or Active/Active, etc.…
Response: 3 total. 2 load balanced and 1 Colocation

Question: What is the speed of the Internet connection at each data center? (100MBps, 500MBps, 1GBps, etc.…)
Response: 5 GIG bursting to 20 @each LB center

Question: Please provide the total number of employees with actual email addresses?
Response: approx 14,000

Question: What is the backend core switching speed? (1GBps, 10GBps, 40GBps, etc.)
Response: 40G

Question: In terms of routing out to the Internet, do all offices/locations go to the Internet through the data centers internet connections?

- The goal here is to inspect all outgoing/incoming traffic, so does all traffic to the Internet go through a choke point like a data center Internet Connection?

- Or does each location/office access the Internet directly, without going through a data center?

Response: Yes. All offices/locations go to the Internet through the data centers internet connections

Question: What are your data retention requirements for telemetry and threat data?
Response: TBD

Question: You mention that the solution should work on-premises and off-premises, can you please provide more detail regarding these requirements?
Response: Many of our staff use laptop computers as their primary workstation and bring them on and off network as needed.

Question: Do you need Remediation actions performed by the MDR solution?
Response: Yes

Question: You mention that you have MDM; do you need mobile threat detection (MTD) and prevention for Chromebooks, iPads, iPhones, and Android devices? Do students/employees take mobile devices off-premises?
Response: No MTD

Question: When you mention "Log Server"; is this a SIEM? Can you please provide your log server platform?
Response: TBD

Question: You mention integration with Active Directory; can you please provide more detail around this requirement?
Response: To be able to monitor any suspicious behavior within Active Directory.

Question: May Aquila bid 2 different solutions?
Response: Please submit a single solution with your best offer.

Question: Are IOS and Android devices in scope?
Response: No.

Question: Are Chromebooks in scope?
Response: No

Question: What Mobile Device Management tool does APS use?
Response: Workspace One

Question: What key controls/technologies are most important to integrate with a new solution?
Response: Log Server, SCCM, Workspace One AD, Azure.

Question: What public cloud environments do you currently use and integrate with?
Response: Azure, Google

Question: How many individuals are on your Security, IT staff, or both?
Response: Approx40

Question: Do you have network segmentation between your student and faculty/staff environments? Any other physical or logical controls as it relates to student vs. faculty/staff you'd care to comment on?
Response: No

Question: What endpoint technologies are in use today?
Response: Malwarebytes, Windows Defender, Trident Lockdown.

Question: Who and which groups make up your cybersecurity team? What outside organizations assist you in your cybersecurity efforts?
Response: This is a shared effort amongst all IT team leaders.

Question: When a cybersecurity incident takes place, who is responsible for handling the escalations?
Response: The first person to identify the incident escalates it to the Executive Director or CIO.

Question: Do you receive threat intelligence feeds today and if so, how are they operationalized?
Response: We have quarterly network scan reports from a third party. Remediation will then be assigned via ITSM integration.

Question: Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?
Response: Yes, our current incumbent may submit a response to this RFP. The expenditures have not yet been calculated.

Question: How many physical locations?
Response: 160

Question: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
Response: Self Managed data centers, third party Colocation.

Question: Are any security products installed? If yes, please provide product name

- Security Incident & Event Management (SIEM)? If yes, which SIEM product name and is it internally or externally managed?
- Endpoint Detection and Response (EDR)

- Vulnerability management
- Email security
- Network threat analytics

Response: Malwarebytes, SCEP, Network Scanning, Phishing and Training Campaign Email security platform.

Question: Can you provide the number of the security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each.

Endpoint

· Number of endpoints?
· Count of Windows/Mac/Linux Desktops/servers (rough)?

Servers: 0

Workstations:
Windows - 11,000
MacOS - 9,000
Total - 21,000

Network

· Number of ingress/Egress Points- 162
· Type of media connectivity - Fiber Optic
· Average and Max Mbps at each Ingress/Egress point - 10 Gbps X2
· High Level network diagram, if available

Email

· How many mailboxes? - 14,000
· Are you currently using Office 365? If so are you using EOP/ATP? - Yes, We still use O365. We have a On Prem/Cloud hybrid setup. Approx 7,000 active users using O365 apps and services. 17,000 Office activations, 3.3mil files in one note.

Current and projected number of users.

· How many network users (at a workstation most of the day)? approx 85,000
· How many users are not on the network most of the day, but authenticate with a domain controller (such as remote workers, maintenance staff, etc)? Very few have an accomodation to work remotely full time and use our VPN service.

Servers/Desktops

· Windows Servers - HIGH EPS (~50 eps)- We do not have a SIEM that calculates this.
· Windows Servers - Low EPS (~2 eps) - We do not have a SIEM that calculates this.
· Windows Workstations (5 / 1k users) - approx 21,000
· Windows AD Servers -20
· Linux Servers - 0
· DNS (enter # per 1000 users) - 6 servers

Network Infrastructure (# of devices)

· Routers 174
· Switches (netflow not supported) 3900
· Wireless LAN 13 controllers / 8613 access points
· Network Load-Balancers 0
· WAN Accelerator 0
· Other Network Devices 5672 IOTdevices surveillance, buildings controls, alarms. 11300 VOIP phones

Security Infrastructure

· Firewall - Internet (Enter # in 1000's of users) - Cisco

· Network Firewalls (Partner / extranets) - None,
· Network Firewalls (DMZ) - Yes we utlize this for aa limited numbe rof services.
· Network IPS/IDS - firepower nexgen fw IDS snort
· Network VPN - Enter # in 100's of users - Dozens of employees not 100o's use VPN.
· Email AntiSpam - Enter # in 100's of users - Gmail
· Network Web Proxy (enter # in 100's of users)none
· Other Security Devices routers w/acls

Applications (Device count assumed with numbers above)

· Web Servers (IIS, Apache, Tomcat) - Unknown-many servers may have IIS setup that don't have WebServer in the machine name.
· Database (MSSQL, Oracle, Sybase - indicate # of instances) - Approx 260
· Email Servers (Enter # in 1000's of users) - We have Exchange for some email use cases but utlize Gmail predominately.
· AntiVirus Server (Enter # in 1000's of users) - Unknown

Other Applications (Email, DB, AV, etc)

Question: What is the approximate budget?
Response: Please submit your best offer.

Question: Do you want a vendor to provide management & monitoring of endpoints in addition to the security software?
Response: Yes.

Question: Do you want to purchase MDR software for your own deployment via the mechanisms identified for deployment in the RFP?
Response: Yes we will deploy after given the appropriate deployment packages.

Question: What are the legacy antivirus and antimalware systems in place?
Response: Malwarebytes, Windows Defender.

Question: If the customer is going to deploy the software themselves, what download software package format will be used - MSI or executable?
Response: MSI is preferred.

Question: When should we expect responses to the written question?
Response: At least five (5) calendar days prior to the RFP due date.

Question: What has been the total expenditure from the district to recover from the recent ransomware attack?
Response: Those expenditures have not yet been calculated.

Question: Please describe the type of cyber-attack- phishing- data stealing? mass encryption? and how it was mitigated.
Response: No proven exfiltration by threat actors. Use of a third party firm in coordination with internal staff to remediate.

Question: How is the MDR solution perceived to be integrated with Albuquerque Public Schools from a response strategy, if something has been compromised?
Response: Integral.

Question: What is your strategy if the Managed Detection and Response solution has been breached and malware starts to rapidly encrypt your data? Security vendors are all in agreement that 100% prevention is not possible 100% of the time
Response: Vendor will be used in accordance with the contract agreed upon to reduce the impact.

Question: In the RFP APS states it reserves the right to multi-award contracts as necessary for adequate delivery. Could the district describe a scenario in which they would award to multiple vendors to support its cybersecurity infrastructure?
Response: That is difficult to determine because APS does not know what offers we will be receiving.

Question: Can you provide an approximate count of servers vs workstations in the APS environment?
Response:

Servers: 0

Workstations:

Windows: 11,000

macOS: 10,000

Total: 21,000

Question: Desired Start Date?
Response: ASAP

Compliance Frameworks		**Number of Firewalls**	
Number of Environments *(number of separate sites, datacenters, AWS/Azure subscriptions or environments, etc.)*	2 data centers and 1 colocation	**Number of Core Switches/Routers** *(typically, one core switch behind each perimeter firewall)*	1 core switch behind a active/standby firewall at each data center
Description of Environments		**Number of External IPs**	16,38 public 11008
Number of Employees *(w/ company emails)*	approx 14,000	**Number of Internal IPs** *(enter number of active internal IP addresses, not CIDR notation)*	*~70,000*

Number of User Endpoints (e.g., laptops/desktops)	21,000	**Number of In-house Developed Web Applications** *(NOT inclusive of 3rd party apps hosted in your environment)*	0
Number of Servers	0	**Description of Security Stack** *(endpoint protection, IDS/IPS, next-gen firewalls, cloud security, etc.)*	Cisco Firepower, Malwarebytes, Windows Defender.
Description of Desired Work			

ACKNOWLEDGE ADDENDUM WITH SUBMITTED PROPOSAL:
Addenda not signed and returned may consider the RFP non-responsive and may be rejected.

_____
COMPANY/FIRM NAME

_____
SIGNATURE

_____
DATE