Warren County School District
Cybersecurity RFP Addendum 1

May 4, 2022

Q1: The requested services can be done remotely, or will you need us on-site? Since you asked for "Physical access controls testing - Determine if the current physical security is effective. Including access to keys, electronic access methods, and logging of access."
R1: Yes, some onsite work will be needed to assess physical infrastructure.

Q2: You need Penetration Testing & Vulnerability Assessments for the whole infrastructure...including testing the 15,000 Private IPs? or it's just posted information. Please let me know the exact scope to size and price it.
R2: Penetration Testing and Vulnerability assessments will include 1 end user device out of the following classes: Student, Staff, Business, classroom display device (ie-SmartBoard), visitor management node, and 1 HR node dedicated for fingerprinting. Testing will be done with 1 device out of each class in addition to server and network nodes as outlined

Q3: Do we need to use a signature, or what are the specific requirements that we need to do with a sealed envelope or box?
R3: The proposal in hardcopy and electronic copy on flash drive or CD must be sealed in an envelope or box which can be hand delivered or sent via carrier if it's received by the deadline. If you would like to use receipt confirmation, feel free to do so.

Q4: The project scope points 11: " Verify that existing user training for identifying phishing emails is effective and that technology measures to limit damage from clicking on a phishing link are appropriate." do you mean you need us to provide sessions or interactive platform for the employees to improve their security awareness?
R4: No you only need to confirm the effectiveness of the programs/processes we currently use.

Q5: What do you mean by " Proposed Contact between the Service Provider and the District." can you give us an example?
R5: This is supposed to read as the proposed **contract**. This is the standard contract you would use for this type of engagement.

Q6: " A single hard copy of these documents AND an electronic copy on a USB drive, CD, or other media must be delivered together in a sealed envelope or box" - should we also send it via Email or only physical mail?
R6: None of the proposals should be sent via email.

Q7: Is there a limit on the financial budget?
R7: We are aware of the significance regarding the cost of providing this type of assessment. We are committed to this project and are willing to seek additional funding if necessary to ensure the success of this project.

Q8: Should we send one technical proposal for the 15 points on the project scope? also, the financial proposal should be one proposal?
R8: Yes- one proposal as long as it encompasses the 15 points on the project scope and the costs for those items.

Q9: Do you need any other papers from our side to be provided other than the ones listed in " Submission Instructions "?
R9: You are welcome to submit additional documentation, but it is not necessary.

Q10: Can we get a high-level network diagram?
R10: A network diagram will be provided after the contract is awarded and signed.

Q11: How many FTE IT staff does Warren County School District (WCSD) have? Please breakdown number by position. (e.g., 1 Network Administrator, 2 DBAs, etc.)
R11: 9
6 Technicians, 1 Technology Systems and Network Administrator, 2 Data Systems Specialist, 1 Technology Coordinator.

Q12: Is all of IT centralized and operating out of a single location or are there departmental IT staff that works independently of central IT?
R12: The IT department is centralized but technicians work within buildings throughout the District.

Q13- How many critical business applications does WCSD use on a day-to-day basis? Which one of these critical applications/services are run/hosted in house? What ones do the outsourced IT support provider provide to WCSD? (e.g., tier 2 problem escalation, firewall monitoring, incident response, etc.)
R13: Eschool, FinPlus – On-Prem & Business Critical, O365/AzureAD - Hybrid Domain. We have no outsourced IT Support other than general support contract/warranty for our applications.

Q14- How many on-premises servers (physical vs virtual) are in place?
R14: 80 virtual, 30 physical.

Q15: How many cloud-based systems do you use and where is each hosted? What are the functions they provide?
R15: Microsoft 365 – AzureAD hybrid domain, outside applications for education hosted by vendor (ie student web-based applications) can be found on our District website.

Q16- How many end user workstations/end points are supported?
R16: Approximately 8000.

Q17- Within WCSD, how many sets of policies and procedures are being used? For IT processes, such as System Patch, Data Security and Backup Security, is there more than one process?
R17: One main technology policy and several procedures that tie back to that policy in a limited capacity. We are looking to develop in-depth policies and procedures in relation to security and recommendations from the service provider.

Q18- How many locations will be in scope for physical access controls testing? Are they in close proximity?
R18: There are 13 buildings within the District and they are all within 20 minutes' drive of each other.

Q19- For the wireless network assessment and penetration testing,
- How many wireless networks (distinct SSIDs) will be in scope?
  R19A: 3
- will there be employees in the office to generate authentication traffic?
  R19B: Yes

Q20- Is private and guest the only wireless networks (distinct SSIDs) that are in scope of penetration testing?
R20: Yes

Q21- Will the SCADA ICS environment be in scope for penetration testing or is only a review of controls required?
R21: Heating control system, lighting control system- Yes

Q22- Do you have any need for web application test and/or API pen test?
R22: No

Q23- For social engineering, what kind of testing do you want to include: phone, email and/or physical site walk-in?
R23: All the above

Q24- For each test, please indicate the number of targets desired.
R24: Penetration Testing and Vulnerability assessments will include 1 end user device out of the following classes: Student, Staff, Administrative Device, Business, classroom display device (ie smart board) visitor management node, 1 HR node dedicated for Fingerprinting, 1 general HR device for testing.

Q25- In the “Re-Assessment” phase, is the assumption that we will re-perform all test work in the first phase after about 30 months?
R25: Yes

Q26- How many firewalls, routers, switches, wireless controllers etc.?
R26: 2 firewalls, no routers, 125 Layer 3 switches, and 1 Wireless Controller (on-prem)

Q27- How many DMZ?
R27: None

Q28- How many wireless SSIDs?
R29: Five wireless networks.

Q30- How are sites connected? MPLS, P2P, VPN
R30: Leased-lit fiber

Q31- Are there any Work from home or Remote users? If so, are they utilizing VPN?
R31: Yes. If they need access to internal resources, they use a VPN.

Q32- Is the capability there to VPN to/from any other 3rd party environment?
R32: Yes

Q33- Is Multifactor enabled?
R33: Yes

Q34- IS SSO enabled?
R34: Yes

Q35- How many ISP providers do you currently have and what services are contracted through them?
R35: One ISP.

Q36- How many firewall rules, policies, NATs?
R36: There are 14 firewall rules. There are three inbound NATs and one single outbound NAT.

Q37- What type of content filtering is enabled?
R37: We use Cisco Umbrella.

Q38- What means do you ensure DNS Security?
R38: Standard Windows DNS setup. DNSSEC is not being utilized.

Q39- Do you have a current IPS/IDS/Antimalware?
R39: No

Q40- Are you looking for 24x7 monitoring/SIEM platform?
R40: No

Q41- Do you have a current MSP?
R41: No

Q42- # of employees/staff with access to confidential/sensitive information
R42: Approximately 12 people.

Q43- # of contractors, third party users, (have direct access to business-critical systems and applications or sensitive data)
R43: 3 Contractors

Q44- # of IT staff
R44: 9

Q45- # of Cybersecurity staff
R45: None dedicated to cybersecurity.

Q46- # of students
R46: Please refer to section 1.1 in the RFP.

Q47- # of Windows Servers
R47: Approximately 70

Q48- # of Linux Servers
R48: Approximately 10

Q49- # of macOS Servers
R49: 0

Q50- # of Windows Devices
R50: Approximately 7,000 with a mix of Desktops/Laptops - Education Edition.

Q51- # of Linux Desktops
R51: 0

Q52- # of macOS Desktops
R52: Approximately 20

Q53- # of Linux Laptops
R53: 0

Q54- # of macOS Laptops
R54: 0

Q55- # of Chromebooks
R55: 0

Q56- # of Printers (networked)
R56: Please refer to section 1.1 of the RFP.

Q57- # of IP phones
R57: Please refer to section 1.1 of the RFP.

Q58- # of IoT devices and types
R58: None to our knowledge.

Q59- Other Operating Systems (exclude appliances)
R59: None

Q60- # of Devices (smartphones and tablets that contain confidential/sensitive information)
R60: Very minimal. Sensitive information is stored online in secure systems.

Q61- Endpoint security solution(s) (e.g., Antimalware, EDR, etc.)
R61: Windows Defender- basic

Q62- Other security solutions
R62: Azure Identity Management (SAML, OATH2, LDAP)

Q63- Storage (NAS, SANs, File Servers)
R63: 2 NAS, 2 File Servers (Clustered)

Q64- External remote access methods (VPN, VDI, Citrix, RDP)
R64: VPN and Azure App Proxy

Q65- # of Firewalls with different configurations (firewall pairs are considered one gateway)
R65: 1

Q66- Web Application Firewalls/DDoS Protections
R66: Yes, DDoS provided on firewall and by ISP.

Q67- Database platforms
R67: SQL x3

Q68- Backup solutions
R68: Veeam and NAS Replication

Q69- Do you have a data flow documented for sensitive information such as ePHI, PII, CUI, confidential, sensitive?
R69: No

Q70- Data center 1 (fully-owned, co-located, cloud IaaS/PaaS/SaaS)
R70: One data center fully-owned.

Q71- Source Code repositories (if you develop applications)
R71: No

Q72- Product Development platforms (if you develop applications)
R72: No

Q73- Financial systems and applications
R73: Yes, we use eFinance for payroll and HR functions.

Q74- Customer Relationship applications
R74: No

Q75- File sharing platforms (SFTP/FTP, OneDrive, Google Drive, SharePoint, etc.)
R75: Yes, we use OneDrive, SharePoint, and SMB.

Q76- Phone systems (not including O365)
R76: Yes, we use a geographically diverse SIPX-COM system.

Q77- Content Management systems
R77: Aptegy

Q78- Learning Management Systems (LMS)
R78: Teams and Buzzagilix

Q79- Sales Commission applications
R79: No

Q80- IT Service Management system
R80: Incident IQ

Q81- Directory Services (e.g., Active Directory)
R81: Active Directory

Q82- Wi-Fi manufacturer
R82: Meraki and Extreme.

Q83- Network routing and switching
R83: Cisco and HP

Q84- Virtualization Platforms
R84: Hyper V

Q85- Other Network Devices (if any)
R85: Cameras, Door Access Controllers, and HVAC controllers. Included in IOT device count in section 1.1 of the RFP.

Q86- Security Awareness & Training solution
R86: BrainStorm

Q87- Vulnerability Management solution
R87: None

Q88- Patch Management solution
R88: WSUS/Endpoint Manager (Intune)

Q89- Asset Inventory solution
R89: Incident IQ

Q90- Active cyber liability Insurance policy (YES OR NO)
R90: Yes

Q91- Last technical vulnerability assessment (or penetration test) covering internal networks and assets AND/OR external-facing networks and assets
R91: Never

Q92: Last cybersecurity program assessment and framework used
R92: None

Q93: Third party IT or Security Audit/Attestation reports (e.g., ISO27001/27002, SOC1, SOC2, SOC3, PCI ROC, NIST CSF, HIPAA, HITRUST, etc.)
R93: None

Q94- Is there a specific objective for this testing (e.g., PCI compliance)?
R94: Please refer to section 1.2 of the RFP.

Q95- How far do you want us to test? If we can bypass the IP's, would you like us to pivot to internal networks, capture a specific target, or stop at the external entry point?
R95: We want to know if you can access sensitive and/or confidential information. At this time we do not know that we need you to pivot.

Q96- We typically perform automated discovery and vulnerability scanning 24x7. Please indicate if other testing windows are required, preference to test during business hours, etc. (Note that non-standard testing windows may impact the overall duration of the penetration test.)
R96: 24x7 testing is fine as long as it does not disrupt District processes and/or education. The District should be notified when testing will be taking place.

Q97- We typically perform manual testing during US daytime hours, but we request the ability to test 24x7. Please indicate if other testing windows are required, preferred, or forbidden. (Note that non-standard testing windows may impact the overall duration of the penetration test.)
R97: 24x7 testing is fine as long as it does not disrupt District processes and/or education. The District should be notified when testing will be taking place.

Q98-We typically perform a single round of post-remediation testing. Please indicate if an alternative approach is appropriate.
R98: Please refer to Item 1.2 in the RFP.

Q99- Does the application have any additional components or functionality such as Flash, HTML 5 Web Sockets, Silverlight, ClickOne, or ActiveX? If so, please provide details about the components.
R99: Once the proposal is awarded and signed this information will be provided.

Q100- Is there a Current Access Control? If so what Manufacturer?
R100: Yes, Bright Blue and Intertech.

Q102- What Level of security card reader is being used?
R102: 26bit

Q103- Is there a need to have Biometric Readers?
R103: No

Q104- Are there currently any MAG locks being used?
R104: Yes

Q105- Are there Request to Exit Buttons or Motion sensors being used.

R105: Yes

Q106- The current Access Control, does it give alert if door is held open for a long period of time?
R106: Yes, but it is not enabled at this time.

Q107- The access control data and access to the program need to be on site or can it be stored in the cloud?
R107: This needs to be on site.

Q108- How many doors need to have access control?
R108: 84 Currently have electronic access control.

Q109- Will access control need to integrate with Video Surveillance system
R109: No

Q110- Is there a need for remote control to open and close doors?
R110: No

Q111- Is there a Current Camera Surveillance System? If so what Manufacture?
R111: Yes. We are currently migrating to one system, Verkada.

Q112- How many Cameras are in Each Building?
R112: Approximately 50

Q113- Are all cameras monitored from one location?
R113: Yes.

Q114- How many monitors and size of monitors will be need to the local monitoring location?
R114: No

Q115- Are current cameras all IP?
R115: Yes

Q116- If there are Analog cameras, do they need to be upgraded to IP
R116: No

Q117- If a camera is to be upgrade to IP, does that require running a new CAT6 line?
R117: No

Q118- Is there POE switches already in use?
R118: Yes

Q119- Is current camera system on a battery back up?
R119: Yes

Q120- Is there a need to multi-channel cameras?
R120: No

Q121- Is there a need for PTZ cameras?
R121: No

Q122- Is there a need to be able to access cameras from and off-site location?
R122: No

Q123- Is there a Current Intrusion System? If so what Manufacture?
R123: Yes – This information will be provided when the proposal is awarded and signed.

Q124- Does the system have any wireless devices?
R124: No

Q125- Does the system use Glass Breaker and Motion sensors?
R125: Both

Q126- Does the system use a standard phone line or Cellular Service to call out?
R126: POTS Lines.

Q127- How many Security keypads are need per building?
R127: None

Q128- How many zones are being used for each security panel at each building?
R128: Single Zone in each building

Q129- How many sirens are being used per building?
R129: None

Q130- Does the Intrusion System need to be integrated into the access control for arming and disarming?
R130: No

Q131- 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?
R131: No

Q132- What's your headcount of users (employees + contractors + interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?
R132: 700 employees and 4000 kids with approximately 5% working remotely.

Q133- How much (%) of the infrastructure is in the cloud?
R133: The only cloud infrastructure are the cloud providers previously mentioned.

Q134- What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?
R134: 10 gbps in 10 buildings, 2 gbps in one building, 20 gbps in one building, and 80 gbps in the data center.

Q135- Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
R135: We manage our own data center.