ADDENDUM 1 QUESTIONS

West Virginia School of Osteopathic Medicine
Cybersecurity & Physical Security Assessment|
RFP# WVSOM-571

Date: March 16, 2026

The purpose of this addendum is to answer questions that have been asked by vendors regarding this bid:

	Question	Answer
1	Would WVSOM require a wireless penetration test as well, or just a wireless security controls assessment would suffice? If wireless penetration test is needed, how many SSIDs or physical sites need to be included?	Yes, WVSOM considers wireless testing to be part of the administrative network scope. There are 3 wireless SSID included in this scope.
2	Should testing be performed on all devices, or would a sample-based approach suffice?	A sample-based approach is fine, but it must incorporate a random sampling of the network that includes different VLANs, device types, and employee types.
3	Are any web or cloud-hosted applications to be found on the public IPs, and are the apps to be included in the external penetration test? If yes, how many apps and what technologies/languages are they written in?	WVSOM expects vendors to include all 40 public IP addresses (30 on-premises and 10 in Azure) in the scope for both the external vulnerability scanning and the external penetration testing. Vendors should assume these IPs host the institutional web servers and VPN appliances.
4	Does the engagement require black box testing, or will credentials be provided for gray/white box testing?	WVSOM requires black box testing for this engagement.

5	Is the use of offshore resources permitted for penetration testing, assuming no data leaves your environment?	No, the use of offshore resources is not allowed.
6	Is there an incumbent currently delivering these services, or is this a new engagement?	There is no incumbent vendor currently delivering these services. This is a completely new contract and initiative.
7	What is the expected timeline for project completion and deliverables?	The vendor is expected to propose the exact timelines. Section 5.3.5 requires the vendor's proposal to include a "detailed five-year engagement schedule" and the "estimated duration (in weeks) for each phase"
8	What is the maximum expected value or budget allocated for this contract?	WVSOM has not set a maximum budget for this project.
9	What specific vulnerability scanning tools or platforms are acceptable to WVSOM, or does the vendor have full discretion over tooling?	Vendors have full discretion over their scanning tools, provided they are non-disruptive and adhere to the criteria outlined in the RFP. Specifically, as stated in Section 4.1, the engagement "shall be non-destructive [and] operationally practical". Furthermore, Section 4.1.2.1.3 reiterates that evaluations must be nondestructive, and explicitly excludes denial-of-service testing and full red team lateral movement exercises.
10	For the Microsoft 365 and Azure Administrative Security Review, will WVSOM provide read-only tenant access, or will the vendor rely on documentation and interview-based review?	Yes, WVSOM is willing to provide read-only accounts to perform the Microsoft 365 and Azure Administrative Security Review.
11	The RFP states approximately 100 servers and 350 workstations. Will the internal vulnerability scan cover all servers and workstations, or will WVSOM define a subset of in-scope assets?	For workstations, a sample-based approach is fine, provided that it incorporates a random sampling of the network that includes different areas. However, WVSOM expects all other devices, servers, and network devices to be fully scanned.

12	Are there any network segments, VLANs, or environments that are explicitly excluded from internal scanning beyond the listed exclusions (Banner Self Service, student-facing systems)?	Yes, WVSOM will list the VLANs to be scanned. The VLANs scanned will be related to employee devices, printers, cameras and technology employees.
13	The RFP states testing must be sensitive to HIPAA and FERPA obligations. Is Securance expected to provide a Business Associate Agreement (BAA) prior to engagement?	
14	Will WVSOM require vendor staff to complete any background checks, FERPA training, or HIPAA training before accessing systems or campus facilities?	See Amendment 1 below. Vendor are expected to current background checks on all personnel members working on this project.
15	How many onsite visit days will be available for the physical security assessment, and who will serve as the WVSOM escort and point of contact during the visit?	There has been no set limit on the number of visit days that will be allowed for a vendor to be on site. Staff who can escort and serve as point of contact will be identified at a later time.
16	What is the expected turnaround time for delivering final reports after data collection is complete for each engagement year?	The vendor is expected to propose the exact timelines
17	Will WVSOM staff be available for structured interviews and document collection during the engagement, and what is the expected time commitment per department or team?	Yes, WVSOM staff from the IT, HR, and Finance departments will be available for structured interviews and document collection. As per Section 5.3.5 of the RFP, the vendor is expected to outline the "Required WVSOM staff participation and estimated time commitments" in their proposal
18	Who is the designated WVSOM IT point of contact for this engagement, and do they have authority to provide access to systems and documentation?	WVSOM will identify this individual at the start of the contract. Yes, the designated point of contact will have the authority to provide access to necessary systems and documentation.

19	Will WVSOM provide a current network diagram, asset inventory, or system documentation to the vendor prior to assessment kickoff?	Yes, WVSOM will provide available network diagrams, asset inventories, and system documentation to the awarded vendor following contract execution and prior to the assessment kickoff.
20	For the Identity and Access Management Review, will WVSOM provide a current Active Directory export or Azure AD user report, or will the vendor need to generate this during the engagement?	WVSOM will provide the current Active Directory export or Azure AD user reports.
21	My company, Enterprise Risk Management, Inc. dba ERMProtect is interested in submitting a response to RFP WVSOM571 (Cybersecurity & Physical Security Assessment). We are reviewing the RFP and would like to confirm that there is no mandatory preproposal/prebid meeting required for this solicitation.	There is no pre-bid required.
22	Is there a proposed timeline for this project? What are the major milestones or events driving the proposed? schedule for the project?	The vendor is expected to propose the exact timelines.
23	Do you have a budget in mind for this project, and can you share that with us? By understanding your budget expectations, bidders can maximize their scope of work within your financial constraints and recommend ways to meet your requirements within your budget.	WVSOM has not set a maximum budget for this project.
24	We conduct our project work using (a) remote videoconference capabilities and virtual tools, to keep expenses down, or (b) by visiting a campus. Which do you prefer?	The Physical Security Assessment is an onsite visit. For all other components, vendors must outline their "onsite vs. remote assumptions" in their proposal
25	Are you willing to share a list of all bidders who have expressed an interest in this project?	Yes, please send a request to legal@osteo.wvsom.edu.

26	If WVSOM exercises the option to hold oral presentations (Section 4.3), would you be willing to consider a videoconference meeting (instead of a face-to-face meeting) to minimize travel expenses?	Yes, if oral presentations are requested by the Agency, virtual meetings via videoconference will be acceptable.
27	May bidders submit proposals covering only a portion of the defined scope of services (e.g., physical security assessment and governance review only), or must proposals address the full scope to be considered responsive?	No. The RFP solicits proposals for a "comprehensive cybersecurity and physical plant security assessment"
28	Will WVSOM accept proposals structured as a prime/subcontractor teaming arrangement, where the prime vendor subcontracts specific technical services, such as active penetration testing or vulnerability scanning, to a qualified specialty firm?	Yes, we need to know the name and contact information of the subcontractor and the services that will be provided by the subcontractor.
29	For the Infrastructure and Network Security Assessment (Section 4.1.2.1.3), may a bidder propose a configuration-based review and analysis methodology in lieu of active vulnerability scanning, provided the deliverables address the same risk findings?	Active vulnerability scanning is required. Section 4.1.2.1.3 explicitly mandates both "External vulnerability scanning" and "Internal vulnerability scanning
30	The required certifications listed in Section 3.6 (Required Documents) and Section 4.2.2.1 are slightly different. Which section is correct? Are the listed certifications required of all personnel on the engagement, or only? those performing active offensive security testing tasks?	Section 3.6 is missing the CISSP (Certified Information Systems Security Professional).
31	For the Physical Security Assessment (Section 4.1.2.1.6), may a bidder propose this component as a standalone engagement separate from the cybersecurity components?	No. The RFP solicits proposals for a "comprehensive cybersecurity and physical plant security assessment"

32	The RFP references HIPAA and FERPA sensitivity (Section 4.1). Will WVSOM require bidders to execute a Business Associate Agreement or Data Use Agreement prior to beginning assessment activities?	WVSOM does not anticipate that the selected vendor will access protected health information (PHI) under HIPAA or education records protected by FERPA as part of the assessment activities. Accordingly, a Business Associate Agreement (BAA) or Data Use Agreement (DUA) is not expected to be required prior to contract execution. However, in the event that the scope of work changes or it becomes necessary for the vendor to access or receive PHI or FERPA-protected data, WVSOM reserves the right to require execution of an appropriate agreement, including but not limited to a BAA or DUA, prior to such access being granted.
33	For the Microsoft 365 and Azure Administrative Security Review (Section 4.1.2.1.4), will WVSOM provide read only administrative access to the tenant, or is the vendor expected to conduct the review through documentation and interviews only?	Yes, WVSOM is willing to provide read-only accounts to perform the Microsoft 365 and Azure Administrative Security Review.
34	Can WVSOM clarify whether "institutionally managed systems" include faculty and staff personal devices enrolled in MDM, or only WVSOMowned endpoints and servers?	No. The scope of this engagement is limited exclusively to WVSOM owned and managed endpoints and servers. Faculty and staff personal devices are not in scope for this project.
35	For internal vulnerability scanning, does WVSOM expect authenticated scans of servers and/or workstations? If so, will temporary credentials or service accounts be provided?	WVSOM will not provide temporary credentials to perform authenticated vulnerability scanning on internal servers and workstations.
36	How many buildings or facilities are expected to be included in the onsite physical security assessment, and are any offcampus or satellite locations within scope?	The onsite physical security assessment is limited to 1 location.

37	The solicitation references submission to the Purchasing Division prior to the bid opening date and time. Could the agency please confirm whether proposals should be submitted via email, physical delivery to the specified address, or if both submission methods are acceptable?	Both email and physical delivery are accepted. This does not require submission to the Purchasing Division.
38	Could the agency please clarify the expected number of key personnel required for this effort and whether there are specific labor categories or roles that vendors are expected to propose for the engagement?	WVSOM does not have a specific number of personnel required for this engagement. Vendors are expected to determine the necessary labor categories and provide their own "proposed staffing plans" in their proposal. Proposed personnel must hold relevant industry certifications appropriate to their assigned role.
39	The solicitation indicates that vendors should provide information such as staff certifications or degrees applicable to the project. Could the agency confirm whether vendors are expected to submit resumes for proposed key personnel and include copies of relevant certifications as part of the proposal?	Resumes are not required.
40	The solicitation lists several acceptable certifications (e.g., CISSP, CISM, OSCP, CEH, CISA, CompTIA Security+ or equivalent). Could the agency clarify whether each proposed key personnel must hold all listed certifications, or whether any relevant certification appropriate to the individual's role would be considered acceptable?	Personnel are not required to hold all of the listed certifications individually or collectively. The certifications listed serve as a baseline for what WVSOM considers valid credentials; we expect the team to hold some combination of those credentials, but we will consider alternatives and equivalents
41	On page 4 of the RFP, the section "Bid Delivery Address and Email" lists both a physical address and an email for submission. Is an email sufficient for the submission of this RFP?	Yes, email is sufficient for the submission of this RFP.
42	On page 4 of the RFP under "Vendor Question Deadline" and "Bid Delivery Address and Email," the email addresses WVSOMbids@osteo.wvsom.edu and bids@osteo.wvsom.edu are listed to submit questions and the final response respectively. Is this difference in email address intentional?	Yes.

43	Per page 6 of the RFP "Exceptions and Clarifications," exceptions to the RFP's terms must be clearly marked. Will WVSOM accept a list of exceptions in a signed transmittal letter?	Yes, as long as the exceptions are clearly identified and reference the RFP section.
44	On page 25, there is a signature line to certify that vendors have reviewed the full RFP. Would WVSOM like this in addition to the signature page on page 29? If so, is the signature page on page 25 to be submitted on its own, or alongside the full RFP?	Yes, please sign both documents. The RFP does not need to be included.
45	Can WVSOM confirm whether the assessment scope includes all Azure subscriptions and Microsoft 365 tenants or only those directly managed by the internal IT team?	The scope includes only the subscriptions directly managed by the internal IT team. Section 4.1.1 states testing focuses "exclusively on institutionally managed systems" and specifically excludes systems outside of WVSOM's direct administrative control
46	For the 100 servers listed in the environment, can WVSOM clarify the approximate breakdown between: o On-premises servers o Azure virtual machines o Platform services (PaaS)?	Of the approximately 100 servers, 85% are in Azure and 15% are on-premises.
47	Does the vulnerability scanning scope include? o Network infrastructure devices (firewalls, switches, VPN appliances)? o Printers and IoT devices?	Yes. The approximately 100 servers, 350 workstations, and 40 network printers listed in Section 4.1.1 are all institutionally managed systems and are in scope for internal vulnerability scanning. For workstations, a sample-based approach is fine, if it incorporates a random sampling of the network that includes different areas.
48	Are third-party SaaS applications integrated with Microsoft 365 or Azure included in the review of identity and access management controls?	No, third-party SaaS applications are not included in this review

49	Can WVSOM confirm whether endpoint security tools (EDR/XDR) currently deployed should be reviewed as part of the security posture assessment?	Yes, endpoint security tools (EDR/XDR) currently deployed should be reviewed as part of the security posture assessment.
50	The RFP states external penetration testing is limited to VPN appliances and institutional web servers. Can WVSOM confirm the approximate number of systems in this scope?	Vendors should assume all 40 public IP addresses (30 on-premises and 10 in Azure) are in scope for the external penetration testing
51	Are authenticated vulnerability scans permitted on internal servers and workstations?	WVSOM will not provide temporary credentials to perform authenticated vulnerability scanning on internal servers and workstations.
52	Are vendors expected to provide manual validation of vulnerabilities identified by automated scanning tools?	Yes, vendors are expected to provide manual validation of vulnerabilities identified by automated scanning tools to ensure accuracy and remove false positives before delivering the severity-ranked findings.
53	Are wireless networks included in the internal vulnerability assessment scope?	Yes. WVSOM considers wireless testing just another administrative network, so it falls under the scope of "Internal vulnerability scanning of administrative networks"
54	Can WVSOM confirm whether the review of Microsoft 365 and Azure security controls includes: o Microsoft Defender security configurations o Microsoft Purview compliance settings o Azure Security Center / Defender for Cloud?	Yes, the review of Microsoft 365 and Azure security controls should include Microsoft Defender security configurations, Microsoft Purview compliance settings, and Azure Security Center / Defender for Cloud.
55	Will the vendor be provided with read-only access to Azure and Microsoft 365 administrative portals, or will assessments rely on documentation and screenshots provided by WVSOM?	Yes, WVSOM is willing to provide read-only accounts to perform the Microsoft 365 and Azure Administrative Security Review.

56	Will WVSOM provide existing policies and procedures for: o Information security o Identity and access management o Incident response o Disaster recovery and business continuity?	Yes, WVSOM will provide existing documentation. Section 4.1.2.1.1 requires the vendor to conduct a Governance and Risk Management Assessment that explicitly reviews information security policies, onboarding/offboarding processes, and disaster recovery planning
57	Are there specific regulatory frameworks currently adopted by WVSOM beyond alignment with NIST CSF (e.g., CIS Controls, HITRUST, ISO 27001)? Does WVSOM currently maintain a risk register or vulnerability tracking system that the vendor should integrate with when presenting remediation findings?	The assessment should be aligned "primarily to the NIST Cybersecurity Framework (CSF)". Services must be sensitive to HIPAA and FERPA, but formal compliance auditing under those specific frameworks is excluded.
59	The RFP indicates a 1–2 day onsite physical security assessment. Can WVSOM clarify the number of buildings/facilities included in scope?	The onsite physical security assessment is limited to 1 location.
60	Will the assessment focus only on IT infrastructure locations, or should it include broader campus administrative areas?	The physical assessment includes both IT infrastructure ("Data Center / Server Environments") and broader Administrative Areas
61	Are existing security system diagrams (badge access, cameras, etc.) available for review prior to the onsite visit?	These will be made available once a vendor has been selected and documentation can be provided prior to the onsite visit.
62	Can WVSOM confirm whether comprehensive assessments (Years 1, 3, and 5) are expected to follow the same scope and level of effort each cycle?	Yes. Years 1, 3, and 5 are designated as identical "Comprehensive Assessments" and require the exact same deliverables

63	Is there a preferred timeframe within each year for when assessments should occur?	While the vendor is expected to propose the exact timelines. Section 5.3.5 requires the vendor's proposal to include a "detailed five-year engagement schedule". In year 1 we will rely on the vendors timelines, going forward we would prefer the engagement in late winter/early spring.
64	Are vendors expected to provide ongoing remediation tracking support between annual assessments?	Ongoing tracking between the annual assessments is not explicitly requested. However, the vendor is required to "Review remediation progress from the prior comprehensive assessment year" during the validation engagements in Years 2 and 4
65	For Years 2 and 4 targeted reviews, should vendors assume the same vulnerability scanning scope as the comprehensive assessments?	Yes, the validation years require the vendor to conduct "updated internal and external vulnerability scans," which implies the same vulnerability scanning scope to validate progress
66	Does WVSOM prefer reports formatted according to a specific template or reporting standard?	Vendors can use their own standard report templates.
67	Does WVSOM will be able to share previously held assessment reports?	Previous assessments have been handled in-house. WVSOM is looking for a new approach for this engagement and will therefore not be sharing previous assessment documents.
68	Should the NIST CSF maturity scoring follow a specific model (e.g., NIST Implementation Tiers, CMMI-style maturity scoring)?	The RFP does not mandate a specific scoring model. Vendors may use their preferred maturity scoring model (such as NIST Implementation Tiers or a CMMI-style model), provided it delivers a clear maturity scorecard with scoring across all five NIST CSF framework functions. This scoring will be used for comparison over the 5 years so the model should remain the same for the length of the contract.
69	For the 12–18-month remediation roadmap, should the vendor include: o Estimated remediation effort o Technology recommendations o Cost estimates?	Yes, the vendor should include all three: estimated remediation effort, technology recommendations, and cost estimates.

70	Are separate technical reports required for each assessment domain (IAM, network, cloud, physical security), or should they be consolidated into one report?	A single, consolidated "Detailed Technical Report" is requested during the comprehensive years, rather than disjointed reports for each assessment domain
71	The RFP requires personnel with certifications such as CISSP, CISM, OSCP, CEH, CISA, or Security+. Can WVSOM confirm whether multiple certifications across the team satisfy the requirement or whether each role must individually hold these credentials?	Personnel are not required to hold all of the listed certifications individually or collectively. The certifications listed in Section 4.2.2.1 serve as a baseline. We expect the team to hold some combination of those credentials, but we will consider alternatives and equivalents.
72	Is there a requirement for onsite personnel during penetration testing or vulnerability scanning activities, or can these be conducted remotely as well?	Vendors must outline their "onsite vs. remote assumptions" in their proposal
74	What are the key specific professionals you are looking for?	WVSOM is not prescribing exact professional roles or a specific number of personnel. Vendors should define the necessary professionals within their proposed staffing plans based on the assessment's scope. As stated in Section 4.2.2.1, WVSOM expects the proposed team to hold relevant industry certifications appropriate to their assigned roles.
75	Will WVSOM provide the equipment to perform vulnerability scanning and assessments?	The vendor is expected to provide their own equipment to perform vulnerability scanning and internal assessments.
76	Should vendors assume travel costs for the onsite physical security assessment are included in the annual lump sum pricing?	Yes, vendors should assume that all travel costs for the onsite physical security assessment must be included in the annual lump sum pricing.

77	For pricing, should vendors assume: o Fixed annual pricing for each contract year o Or pricing escalation across the 5-year contract term?	Vendors should provide fixed annual pricing. Attachment A asks for a "Lump Sum Annual Price" for each of the 5 contract years, allowing vendors to factor in their own pricing escalation
78	Can WVSOM confirm whether the targeted validation years (2 and 4) should be priced lower than comprehensive assessment years?	While the scope of work for the Targeted Review and Validation in Years 2 and 4 is significantly narrower than the Comprehensive Assessments ,leading to the general expectation that those years would be priced lower, WVSOM does not dictate the pricing structure. It is up to the vendor to determine and propose their own Lump Sum Annual Price for each individual contract year, as outlined in Attachment A: Cost Sheet.
79	What's the budget for this project?	WVSOM has not set a maximum budget for this project.
80	What are the submission criteria cause in the ad document you have mentioned that it's an email submission but there is an option to submit the proposal into wvoasis.gov portal?	Proposals can be submitted electronically via email to bids@osteo.wvsom.edu or via physical delivery
81	Is it mandatory to accept P-Card option or electronic funds transfer would be fine?	Electronic Fund transfer is acceptable.
82	If oral presentations are requested, will they be conducted in person or virtually?	Yes, if oral presentations are requested by the Agency, virtual meetings via videoconference will be acceptable.
83	What is the initial project starting date and the award date?	WVSOM intends to award the contract and begin the Year 1 engagement in the Fall but the vendor can make suggestions. For Years 2 through 5, WVSOM prefers a late winter or early spring engagement start time. As per Section 5.3.5 of the RFP, vendors should outline their proposed schedules accordingly.

84	Has WVSOM previously conducted similar cybersecurity or physical security assessments? If so, are the resulting documents available to the awarded vendor?	Previous assessments have been handled in house. WVSOM is looking for a new approach for this engagement and will therefore not be sharing previous assessment documents.
85	Are there any incumbent vendors currently providing cybersecurity or related IT services to WVSOM? If yes, please provide their names and scope of work.	There is no incumbent vendor currently delivering these services. This is a completely new contract and initiative.
86	Are there specific recurring pain points, challenges, or security incidents that WVSOM would like this assessment to prioritize?	No, there are no specific pain points or incidents to prioritize. Vendors should stick to a general baseline assessment.
87	Have any recent security events, audits, or assessments identified specific areas of concern requiring deeper examination?	No, there are no specific areas of concern requiring deeper examination. Vendors should stick to a general baseline assessment.
88	Is there any page limit for technical proposal?	There is no page limit specified. Section 5.1 only states that proposals should be "prepared simply and economically"
89	Does your environment include any directories outside of Active Directory—for example, Google or other identity platforms?	No, WVSOM only uses Active Directory and Azure AD.
90	Printers are mentioned as part of the device assessment, but are there any non-standard devices connected to the network, such as IoT/OP devices - If so, how many?	Yes, there are non-standard IoT devices on the network. Rather than an exact count, vendors should plan to assess a sampling of different device types, such as UPS systems, security cameras, and digital signage.
91	Is there a single group responsible for GRC? - If no, how many different GRC groups exist and what specific operations do they oversee?	There is no dedicated GRC department. Governance, risk, and compliance responsibilities are a collaborative effort overseen by IT Leadership, the Infrastructure team, and relevant institutional departments.

92	How many individuals will be subject to interviews to support the NIST CSF maturity assessment?	Interviews should include staff from the IT, HR, and Finance departments. The exact number of individuals will depend on the vendor's proposed methodology; vendors must include their estimated staff participation requirements in their proposal (Section 5.3.5)
93	How many management teams oversee Cloud (M365/Azure) operations?	There is one team managing both M365 and Azure operations.
94	Can one or two read-only Cloud accounts with API and Portal access be provisioned to perform the Cloud security assessment?	Yes, WVSOM is willing to provide read-only accounts to perform the Microsoft 365 and Azure Administrative Security Review.
95	Of the 100 servers, how many are internet facing institutional web servers?	Vendors should assume the 40 public IP addresses encompass the in-scope internet-facing VPN appliances and institutional web servers
96	For institutional web servers, is checking for known vulnerabilities sufficient (COTS) or should unauthenticated web application assessments be conducted to identify vulnerabilities in custom code?	Both are required. Vendors should conduct known vulnerability scanning as well as unauthenticated web application penetration testing on these 40 public IPs to identify vulnerabilities. However, testing must adhere to the limitations in Section 4.1.2.1.3 (it must be nondestructive, exclude DoS, and exclude lateral movement)
97	Can the internal administrative networks be reachable from a single network port? - If no, how many different network ports are required to conduct scanning and testing activities from?	Yes, the internal administrative networks can be reachable from a single network port. WVSOM can configure this as a trunk port, allowing the vendor to update their IP and VLAN tags as needed during testing.
98	For internal scanning, can the tests be conducted remotely via a vendor-provided jump box device or a WVSOM-provided VM via VPN, or is on-site testing required?	Yes, the internal scanning tests can be conducted remotely via a vendor provided jump box. The vendor is expected to provide their own equipment to perform vulnerability scanning and internal assessments.
99	Can our scanning devices (laptop/jump box) be configured with unrestricted Internet access? (Potentially allow-listing it from NAC, web proxy, and NIPS security controls during the assessment)	Yes, WVSOM can accommodate this. The vendor will need to provide the device MAC address and a brief tool description in advance. The exemption will be scoped exclusively to that device for the duration of the assessment only.

100	Is separate vulnerability assessment and scanning from Azure required, or are Azure hosts accessible from on-prem?	No separate vulnerability assessment and scanning from Azure is required; Azure hosts are accessible from on-prem.
101	How many security boundaries or network segments are required for segmentation review (i.e., how many "from source network X to destination network Y" tests must be conducted?)	Vendors should assume testing approximately 10 internal network segments or VLAN boundaries. The specific boundaries and pathways will be identified with the awarded vendor during project kickoff.
102	How many firewall configurations require review? - Can a read-only login be provided to access its console?	There are 2 firewalls requiring configuration review.
103	How many VPN configurations require review? - Can a read-only login be provided to access its console?	There is 1 VPN requiring configuration review.
104	How many AD forests and domains are in scope?	There is 1 Active Directory Forest in scope.
105	What access control (e.g., IAM/PAM/PIM) systems/tools are in use?	Active Directory and Azure are used for IAM.
106	What license is M365 and Azure?	WVSOM utilizes Microsoft 365 A5 and Azure AD Premium P2.
107	How many different end-point protection configurations are required for review?	There is one standard endpoint protection configuration required for review.
108	How many different Azure Virtual Desktop configurations are required for review?	There are two different Azure Virtual Desktop configurations required for review.

109	How many different M365 Backup and Recovery configurations are required for review?	There is one M365 backup and recovery configuration required for review.
110	Is the Physical Security Assessment to be conducted solely at the main campus or is travel to other locations required? - If other locations are required, how many?	The onsite physical security assessment is limited to 1 location.
111	Does the 4.1.2.2 Targeted Review (years 2 and 4) include reassessment for: * All of 4.2.1.1.* - if so, is verbal confirmation or documentation review of a security control's remediation implementation acceptable for validation that year or is configuration review or testing required for changed controls when applicable? * All of 4.1.2.1.3? * Only 4.1.2.1.3's external and internal vulnerability scanning line items?	For validation of remediated controls (referencing 4.1.2.1.1), verbal confirmation is not sufficient; WVSOM requires configuration review or testing/evidence to validate that changed controls were successfully remediated. Regarding 4.1.2.1.3, as noted in Section 4.1.2.2 and Question 65, vendors must conduct full, updated internal and external vulnerability scans. For the remaining items in 4.1.2.1.3, vendors only need to perform configuration reviews on infrastructure or controls that have changed or were flagged for remediation during the prior comprehensive assessment.
112 113	Would you like us to include a Wireless Security Assessment since in-scope "Physical" and "Internal" threats often exploit wireless? - If so, how many wireless SSIDs are in scope, and can this be performed remotely with a vendor-provided jump box device, or is on-site testing required? Are the 30 public IP addresses on premises and the 10 public IP addresses in Azure all in scope for the external vulnerability scanning?	Yes, WVSOM considers wireless testing to be part of the administrative network scope. There are 3 wireless SSIDs included in this scope . Yes, all 40 public IP addresses are in scope for both external vulnerability scanning and external penetration testing

114	Similarly, are the 100 servers, 350 workstations, and 40 network printers all in scope for internal vulnerability scanning? Or are there other network devices expected to be in scope?	Yes. The approximately 100 servers, 350 workstations, and 40 network printers listed in Section 4.1.1 are all institutionally managed systems and are in scope for internal vulnerability scanning
115	In section 4.1.2.1.3 Infrastructure and Network Security Assessment, both external vulnerability scanning and external penetration testing are mentioned. Are we to interpret this as WVSOM expects these pieces separate from each other? (Usually, an external vulnerability scan is part of the external penetration testing process.)	Yes, while WVSOM understands that an external vulnerability scan is typically part of the penetration testing process, we expect both pieces as distinct evaluation requirements so that we receive comprehensive vulnerability reporting alongside the active exploitation results.
116	Is wireless network penetration testing expected to be in scope? If yes, what is the number of distinct SSIDs that will be in scope?	Yes, WVSOM considers wireless testing to be part of the administrative network scope. There are 3 wireless SSIDs included in this scope
117	What is number of IT staff at WVSOM?	WVSOM has approximately 20 IT staff members.
118	Is any aspect of IT operations outsourced to a third-party service provider? (e.g., network/system monitoring, DR site, log analysis, etc.)	No, WVSOM does not currently outsource IT operations to a third-party service provider.
119	What is the expected timing for the engagement start?	WVSOM intends to award the contract and begin the Year 1 engagement in the Fall but the vendor can make suggestions. For Years 2 through 5, WVSOM prefers a late winter or early spring engagement start time. As per Section 5.3.5 of the RFP, vendors should outline their proposed schedules accordingly.
120	Is it the preference of WVSOM that fieldwork be conducted in-person and onsite?	The Physical Security Assessment is an onsite visit. For all other components, vendors must outline their "onsite vs. remote assumptions" in their proposal

121	What is the budget that the WVSOM has allocated for this engagement?	WVSOM has not set a maximum budget for this project.
122	Is this a new initiative of the School of Osteopathic Medicine or offered at renewal of a previously contract for similar 5 year cyber and premise security engagements and if so, do you expect that incumbent to also bid?	There is no incumbent vendor currently delivering these services. This is a completely new contract and initiative.
123	Regarding Section 4.1.2.1, *Project Deliverables*, what content is expected in the detailed technical report?	Expected report content is dictated by the deliverables requested for each technical domain (Governance, IAM, Infrastructure, Cloud, and Physical) outlined in Sections 4.1.2.1.1 through 4.1.2.1.6
124	Regarding Section 4.1.2.1.1, *Government and Risk Management Assessment Deliverables*, there is a request for a maturity assessment as well as identification of control gaps. Does WVSOM have a documented NIST CSF target profile that should be used to identify gaps, or are gaps strictly considered areas where controls are not implemented?	WVSOM does not currently have a documented NIST CSF target profile. For this initial assessment, gaps should be considered areas where baseline controls are not implemented or are immature. The vendor's recommendations will help WVSOM establish a target profile moving forward.
125	Regarding the request for benchmarking, how many peers should be included in this exercise, have peer institutions been identified, and are there established relationships with these peers?	WVSOM has not identified specific peer institutions for this exercise and does not have established data-sharing relationships for this purpose. Vendors should utilize their own industry data to benchmark WVSOM against a general sample of similar higher education or healthcare institutions (e.g., 3-5 peers).
126	Section 4.2.2, *Mandatory Qualification/Experience Requirements*, subsection 4.2.2.1 states that "Proposed personnel assigned to this engagement shall hold relevant industry certifications appropriate to their role. Acceptable certifications include, but are not limited to: •CISSP (Certified Information Systems Security Professional) •CISM (Certified Information Security Manager) •OSCP (Offensive Security Certified Professional)	Personnel are not required to hold all of the listed certifications individually or collectively. The certifications listed in Section 4.2.2.1 serve as a baseline for what WVSOM considers valid credentials. We expect the team to hold some combination of those credentials, but we will consider alternatives and equivalents.

	•CEH (Certified Ethical Hacker).” Does WVSOM expect the proposed team to collectively hold the four certifications specified in the RFP, or will a subset of these four certifications along with other relevant industry certifications suffice?	
127	Does WVSOM require the vendor to include digital copies of the proposed team’s certifications with the proposal submission?	Yes. Section 4.2 specifically asks vendors to provide "copies of any staff certifications or degrees applicable to this project"
128	Will WVSOM confirm that vendors may submit their bids electronically in PDF or Word format to the email listed in *6. Bid Submission*?	Proposals can be submitted electronically via email to bids@osteo.wvsom.edu or via physical delivery
	Amendment 1 – Background check	The Vendor shall ensure that all personnel assigned to perform services under this agreement have successfully completed a criminal background check within the previous twelve (12) months. Upon request, the Vendor shall certify that such background checks have been completed. WVSOM reserves the right to require removal of any personnel deemed unsuitable.