Consolidated Questions and Responses

RFP No. 26-IT-001

Managed IT Services, Cybersecurity Operations, and HIPAA Security Program Management
Williamson County Children's Advocacy Center (WCCAC)

Contents

1. Procurement Timeline, Transition, Incumbent Provider, and Proposal Requirements

2. Environment, Hardware, Network, Facilities, and Asset Inventory

3. Microsoft 365, Identity, Devices, Email, and Licensing

4. Managed IT Support, Help Desk, Remote Work, and Onsite Services

5. Security Monitoring, SOC/MDR, Incident Response, and Cyber Insurance

6. Backup, Recovery, Vulnerability Management, and Penetration Testing

7. HIPAA Security Program, PHI/PII, Access Controls, and Compliance

8. Applications, SaaS, Vendors, Subcontractors, Personnel, and CJIS

9. Governance, Service Levels, Pricing, Insurance, and Contract Terms

1. Procurement Timeline, Transition, Incumbent Provider, and Proposal Requirements

Question 1

Is a virtual call available before October 23? WCCAC is not planning individual calls prior to the proposal deadline. Respondents should prepare their proposals based on the information provided in the RFP and written clarifications and clearly identify any assumptions used in developing their proposed approach and pricing. The selected vendor will participate in a structured discovery and assessment process following award and contract execution, at which time WCCAC can provide appropriate access to additional technical information, documentation, and the environment.

Question 2

Please describe the current state of WCCAC's HIPAA Security Program, including whether a risk analysis, security policies, or a remediation tracker already exist and when they were last updated, and identify all systems and applications that create, store, or transmit ePHI (for example, case management, forensic interview recording, and other cloud applications) that the vendor's risk analysis is expected to cover. WCCAC has a HIPAA Risk Assessment conducted annually. We conduct quarterly security training through KnowBe4 and we have all staff complete annual HIPAA training. We have a POA&M and a remediation tracker that are reviewed monthly. PHI/PII is transmitted through multiple systems to include case management, forensic interviewing, cloud based storage for medical, and other various platforms. We have MFA and/or password protections on our systems. During the discovery phase, we will be able to provide the assessment and POA&M to show progress.

Question 3

Will the incumbent provider support the transition, including timely transfer of documentation, credentials, licensing, configurations, and knowledge? Yes, we have a MSP that currently provides these services. We anticipate the current provider to assist with the transition, if needed. WCCAC will coordinate any knowledge transfer.

Question 4

Can WCCAC accommodate a brief technical site visit or structured discovery meeting before the proposal deadline, subject to its procurement rules? WCCAC is not planning individual technical site visits or discovery meetings prior to the proposal deadline. Respondents should prepare their proposals based on the information provided in the RFP and written clarifications and clearly identify any assumptions used in developing their proposed approach and pricing.

The selected vendor will participate in a structured discovery and assessment process following award and contract execution, at which time WCCAC can provide appropriate access to additional technical information, documentation, and the environment.

Question 5

Can you provide a detailed and current asset inventory, including:

1. **Workstations and laptops approx.** 75
2. **Servers (physical and virtual)** 0 for systems; 2 for forensic interview system (closed system)
3. **Network devices** 3 switches, 1 VPN
4. **Firewalls** 1
5. **Wireless access points** 33

6. **Printers** 7
7. **Mobile devices** 1 – we manage the remainder of our mobile devices in-house other than 1

Any cloud-hosted assets

Question 6

Following onboarding and transition, what ongoing operational responsibilities are expected from the selected provider? Yes, we expect onboarding and offboarding support.

Question 7

Are there any existing operational runbooks, standard operating procedures, or support documentation that will be transitioned to the selected provider? Yes, we have these documents that will transfer.

Question 8

If yes, what portions of the current environment and operations are managed by the incumbent provider today? Our MSP currently handles the majority of our systems and/or helps to coordinate the service of our systems.

Question 9

Could WCCAC kindly extend the proposal due date by 1-2 week? We are not able to extend as we receive grant funding and need to have a contract in place.

Question 10

Please clarify whether WCCAC has specific requirements for professional staff, including minimum staffing levels, dedicated personnel, qualifications, certifications, and roles and responsibilities for this contract. WCCAC has not established minimum staffing levels or required dedicated personnel for this contract. Respondents should propose a staffing model appropriate to meet the service, security, compliance, response-time, and reporting requirements of the RFP.

Respondents should identify the key roles assigned to the engagement, their responsibilities, relevant qualifications and certifications (such as CJIS), availability and escalation coverage, and any subcontractors supporting the services.

WCCAC will evaluate the proposed staffing approach as part of the respondent's overall ability to meet the requirements of the RFP.

Question 11

Do you have a page limit or preferred format for the narrative, beyond completing Attachments A through J? WCCAC has not established a formal page limit for proposals. However, respondents are encouraged to provide clear, concise, and well-organized responses that directly address the requirements of the RFP.

In addition to completing Attachments A through J, respondents should provide sufficient detail for WCCAC to evaluate their qualifications, technical approach, service model, and pricing. Marketing materials and supplemental documentation may be included as appropriate but should be relevant to the services proposed.

WCCAC encourages respondents to focus on quality and clarity of information rather than volume of content. Executive summaries, tables, diagrams, and other concise formats are welcome where they improve readability and understanding.

2. Environment, Hardware, Network, Facilities, and Asset Inventory

Question 12

Are all devices Windows-based? Are they Windows Pro? All of our laptops are Dell (various models), with the exception of one (MAC) in use and 5 mini-PCs (Beelink).

Question 13

Are there any company-owned tablets or phones that require management? We have one iPad that is part of the forensic interview system that requires management. We have other iPads that are managed by WCCAC.

Question 14

What is the brand and model of the firewall, Switches, and access Points? Our Firewall and switches were recently replaced. Our WAPs were installed in 2023 during the expansion of our facility. Our network printers are on a lease, and we utilize a VPN.

We utilize Firewall: Zyxel USG Flex 500H, Switches: Zyxel GS1920-48HP, WAP: Ubiquti UAP.

Question 15

How many VLANs are currently in place and operational? WCCAC believes the current network includes approximately two VLANs and one VPN connection; however, these configurations have not been independently validated for purposes of this solicitation.

The selected provider will be expected to validate the existing network segmentation, VLANs, VPN configuration, firewall rules, and remote-access requirements during the discovery and network assessment. Respondents should identify any assumptions or recommended changes in their proposal.

Question 16

Are the network printers under a service contract with a printer vendor? We have a lease and service contract for the majority of our printers. Our MSP does assist us to coordinate connectivity and troubleshooting issues.

Question 17

Does the organization have a single or multiple internet providers? Who are the providers? We have one ISP that is provided by Williamson County.

Question 18

Are phones/VoIP, security cameras, door access control, conference room AV, or mobile devices in scope? Our phone system, door access and security cameras are managed by Williamson County and not WCCAC. Our AV systems are currently on a service contract, although we may need assistance with technical support on occasion.

Question 19

Please share average monthly ticket volume for prior 12 months. We have approximately 40 tickets per month on average.

Question 20

Are there any planned technology refreshes, migrations, or major infrastructure changes anticipated during the contract period? We have all our systems on a replacement schedule for hardware refresh. We anticipate laptop refresh annually and possibly a new forensic interview system update prior to the contract end date.

3. Microsoft 365, Identity, Devices, Email, and Licensing

Question 21

Are there any local servers on site? WCCAC is mostly virtual using Microsoft 365. We do have 2 physical servers for our forensic interview system. Our forensic interview system is managed by WCCAC with assistance from our MSP for technical issues. We have service contracts and we anticipate some MSP assistance on these services for system updates.

Question 22

How is the organization protecting the email system? Do you use a third-party email protection system? Microsoft Defender? WCCAC currently has email security and protection controls in place within its Microsoft 365 environment; however, specific products and configurations are not being disclosed as part of this solicitation.

Respondents should propose the email security protections they recommend as part of their solution and clearly identify any required Microsoft licensing, third-party products, additional costs, or assumptions. The selected provider will be expected to review and validate the existing email security configuration during the discovery and security assessment.

Question 23

How many user accounts are in the Microsoft O365 tenant? We have about 60 accounts in Microsoft.

Question 24

Is the organization paying for the Microsoft O365 Tenant directly (to Microsoft)? WCCAC purchases each license as we utilize a non-profit version of Microsoft 365 E3. We are able to make our purchases and utilize recommendations from our MSP.

Question 25

Does WCCAC currently use Intune, Defender, SharePoint, OneDrive, and Teams? If not, which alternatives are used for device management, endpoint security, and collaboration? WCCAC uses Microsoft 365 SharePoint, OneDrive, and Teams. Our current MSP may use other endpoint systems.

Question 26

Is MFA enforced for Microsoft 365 and other critical systems? Which identity/MFA solution is in place? Yes, we utilize an MFA for our systems through Microsoft.

Question 27

The RFP references 24x7 SOC services and continuous security monitoring. Can you confirm whether the expectation is:

WCCAC's expectation is full managed detection and response, including 24x7 monitoring, alert triage, investigation, escalation, response coordination, and appropriate containment or remediation actions based on established authorization and escalation procedures.

Respondents should clearly describe which response actions their SOC is authorized to perform directly, which require WCCAC approval, and how critical incidents will be communicated and escalated after hours.

4. Managed IT Support, Help Desk, Remote Work, and Onsite Services

Question 28

How many support requests are generated in a typical month? We average about 40 tickets per month.

Question 29

Are all of your staff on-site? We have one remote employee locally (Williamson County) and we allow some employees to work remote on occasion.

Question 30

Is there a camera system on-site? If so, is it in scope of the requested support services? We do have a camera system on site. It is managed by Williamson County and not included in the scope of the MSP.

Question 31

Part VII applies screening and training to staff with physical or logical access. Does this encompass all remote service desk, engineering, NOC, and SOC personnel who may administer WCCAC systems, or only specified roles/access levels? What evidence and approval process is required before access? WCCAC recognizes that

certain subcontractor personnel, such as remote SOC analysts, may not require physical access to WCCAC facilities and may have limited logical access necessary to perform monitoring functions. For such personnel, WCCAC will consider documented background screening and HIPAA training provided by the subcontractor in lieu of SafeSport training and sex-offender registry checks, provided the respondent clearly describes the personnel's role, level of access, and applicable safeguards.

Any personnel with physical access to WCCAC facilities, access to sensitive systems, or access beyond what is necessary to perform monitoring functions will be subject to the full screening and training requirements outlined in the RFP.

Respondents should describe their proposed access model and provide sufficient information for WCCAC to evaluate the appropriateness of any alternative screening or training approach.

Question 32

What is the expected onsite support frequency (scheduled visits and incident dispatch), and are there specific onsite arrival-time or emergency response expectations beyond the ticket acknowledgment SLAs? WCCAC currently receives regularly scheduled onsite support approximately one day per week. While WCCAC has not established a required minimum number of onsite hours under this solicitation, respondents should propose the level of onsite support they believe is appropriate to effectively support the environment and clearly identify any included onsite hours, response expectations, travel policies, and associated costs.

WCCAC's regular operating hours are generally 8:00 a.m. to 6:00 p.m. Central Time. In addition, because WCCAC supports services and operations that may extend beyond normal business hours, respondents should

describe their after-hours support capabilities and procedures for responding to critical incidents, service disruptions, and security events requiring 24x7 coverage.

WCCAC expects most routine help desk functions to be provided during business hours, with escalation and emergency-response capabilities available outside of normal operating hours. Respondents should clearly describe their proposed help desk hours, after-hours support model, escalation procedures, and any assumptions used in developing their pricing.

Question 33

What percentage of support requests typically require onsite assistance? WCCAC does not track a specific percentage of support requests requiring onsite assistance. Most support needs can be handled remotely; however, WCCAC has found that regularly scheduled onsite support, currently approximately one day per week, is an efficient way to address help desk items and other issues that benefit from in-person assistance.

Respondents should propose an appropriate mix of remote and onsite support and clearly identify the onsite support included in their pricing.

Question 34

Is there a required onsite response time or minimum scheduled onsite presence? While not required, we currently have a person one day a week on site and that has been beneficial to move projects and coordinate help desk items.

5. Security Monitoring, SOC/MDR, Incident Response, and Cyber Insurance

Question 35

Does the client currently have Cybersecurity insurance regulations they need to abide by? WCCAC maintains cyber insurance. The selected provider will be expected to cooperate with WCCAC in meeting applicable security, incident reporting, documentation, and response requirements associated with its cyber insurance coverage. Specific policy terms and requirements are not being provided as part of the solicitation. In the event of a security incident, the selected provider will be expected to coordinate with WCCAC and, as applicable, its insurance, legal, forensic, and other incident-response resources.
Respondents should describe their standard incident-response and reporting processes and identify any assumptions or requirements relevant to supporting a cyber-insurance-related incident.

Question 36

What endpoint, email, network, and security-monitoring products are in use today, and which existing subscriptions or contracts are expected to continue? We utilize Microsoft and that is expected to continue.

Question 37

Are there any existing SIEM, log management, or security monitoring platforms currently deployed? WCCAC currently has security monitoring and endpoint management capabilities in place. However, respondents should not assume that existing SIEM, log management, or security monitoring platforms will transfer to the selected provider.

Respondents should propose the tools and platforms necessary to deliver the required 24x7 SOC/MDR services and clearly identify any associated licensing, dependencies, or assumptions. The existing environment will be further validated during the post-award discovery phase.

Question 38

What log sources are expected to be included within the monitoring scope? WCCAC expects the monitoring scope to include, at minimum, endpoints, Microsoft 365, firewall and network security devices, identity/authentication events, and other security-relevant log sources necessary to provide the proposed 24x7 SOC/MDR service. Respondents should clearly identify the log sources included in their proposed solution, along with any licensing, configuration, or other dependencies.

Question 39

What incident-response responsibilities are expected from the selected provider versus customer personnel? The selected provider is expected to provide incident monitoring, triage, investigation, containment and remediation support, escalation, and response coordination. The provider should take appropriate technical response actions within agreed-upon authorization levels and immediately notify WCCAC of significant or critical incidents.

WCCAC personnel will be responsible for organizational decisions, internal communications, and coordination with leadership, legal counsel, insurance, law enforcement, regulatory agencies, or other external parties as appropriate. The selected provider will be expected to provide technical information and assistance necessary to support those activities.

Respondents should clearly describe their incident-response model, including actions they can take without prior approval and actions requiring WCCAC authorization.

Question 40

Is the provider expected to perform containment and remediation activities, or only investigation and escalation? The selected provider is expected to perform investigation, containment, remediation support, and escalation, not solely investigation and notification.

Respondents should clearly describe which containment and remediation actions can be performed directly under established authorization procedures and which actions would require WCCAC approval. Critical incidents should be promptly communicated and coordinated with WCCAC.

Question 41

Section 8 calls for 24x7 Security Operations Center coverage. Would WCCAC accept a SOC delivered through a disclosed, approved subcontractor under Attachment C, with the prime respondent remaining fully responsible? Yes. WCCAC will consider proposals that utilize a subcontractor to provide 24x7 SOC services, provided the subcontractor is fully disclosed in Attachment C and the respondent clearly identifies the roles and responsibilities of all parties.

The prime respondent will remain fully responsible for contract performance, service delivery, security, compliance, reporting, incident response coordination, and all other requirements of the RFP, including those performed by subcontractors.

Respondents should describe the subcontractor's experience, services provided, staffing model, and any applicable security, compliance, and reporting capabilities as part of their proposal.

Question 42

SOC scope. Beyond endpoints, Microsoft 365 and the firewall, are there other log sources the 24x7 SOC should cover? Which Microsoft 365 license tier is in use, and is any endpoint protection or SIEM in place today? For proposal purposes, respondents should assume 24x7 SOC monitoring will, at a minimum, include endpoints, Microsoft 365, firewall/security devices, and other security-relevant systems and log sources customarily monitored as part of a managed security service.

WCCAC has not provided a comprehensive inventory of current log sources, security tools, license levels, endpoint protection platforms, or SIEM technologies as part of this solicitation. Respondents should describe their

proposed monitoring scope, data sources, assumptions, and any prerequisites necessary to deliver the proposed SOC services.

The selected vendor will be expected to validate the environment during the discovery phase and provide recommendations regarding log-source coverage, security monitoring architecture, retention requirements, endpoint protection, and SIEM capabilities necessary to support WCCAC's security and compliance objectives.

Where a respondent's proposed solution depends upon specific Microsoft 365 licensing levels, endpoint security products, or SIEM platforms, those assumptions should be clearly identified in the proposal, along with any associated costs or upgrade recommendations.

6. Backup, Recovery, Vulnerability Management, and Penetration Testing

Question 43

What is the current tempo for penetration testing? Quarterly

Question 44

What solutions currently protect Microsoft 365 data and any server or SaaS data? Are backups tested, and are recovery objectives documented? Backup and recovery services are within the scope of this solicitation.

WCCAC is seeking respondents' recommendations regarding the appropriate approach for protecting Microsoft 365, endpoints, and other in-scope systems.

Respondents may propose support for existing backup and recovery capabilities, enhancements to those capabilities, or alternative solutions. Any assumptions regarding existing tools, retention periods, recovery objectives, licensing, or service ownership should be clearly identified in the proposal.

Where backup services, Microsoft 365 backup, endpoint backup, disaster recovery, or related technologies are not included in the respondent's base offering, those items should be clearly identified along with any associated costs.

The selected vendor will be expected to validate the backup and recovery environment during the discovery phase and provide recommendations necessary to support WCCAC's operational, security, business continuity, and recovery requirements.

Question 45

May annual penetration testing, onsite tabletop facilitation, and other clearly scoped annual services be separately itemized in the pricing schedule, while maintaining full visibility into total cost? Yes. Clearly scoped annual services, such as penetration testing and onsite tabletop exercises, may be separately itemized in the pricing schedule. Respondents should clearly identify the frequency and cost of each service so WCCAC can evaluate the total cost over the full contract term.

All required services and associated costs should be disclosed in the proposal.

Question 46

Are tabletop exercises, incident-response plan reviews, or security testing activities currently performed, and at what frequency? We conduct 2 tabletops a year, review incident response quarterly, and conduct security testing activity quarterly at a minimum.

Question 47

Pricing and contractual terms: Should proposed pricing assume all endpoint and security licensing and ongoing independent testing costs are included? Respondents should include in their pricing all licensing, services, and recurring costs that are necessary to deliver their proposed solution. If endpoint security licensing, backup services, SOC services, penetration testing, vulnerability management, or other security-related costs are

not included in the base proposal, those items should be clearly identified along with any associated costs and assumptions.

Question 48

Penetration testing. Under Part IV, Section 10, does a separately staffed security team within the respondent qualify as "appropriately segregated," or must an outside firm perform the annual test? Yes. For purposes of this solicitation, an annual penetration test performed by a separately staffed and operationally independent security team within the respondent's organization may satisfy the "appropriately segregated" requirement. An outside firm is not required, provided the respondent clearly describes the independence of the testing team, testing methodology, quality controls, and reporting process.

Respondents should disclose whether penetration testing is performed by internal personnel, a separate business unit, a third party, or a subcontractor.

Question 49

Annual penetration testing. Part IV, Section 10 requires at least annual testing, while Attachment A lists only initial internal and external tests as one-time costs. Should repeat annual testing be included in recurring pricing, or priced as a separate annual line item? Annual penetration testing should be included as part of the respondent's overall pricing approach for the contract term. Because WCCAC requires at least annual penetration testing, respondents may either include recurring annual testing costs within their monthly recurring pricing or identify them as a separate annual line item, provided the pricing methodology is clearly described.

Attachment A includes initial internal and external penetration testing as one-time implementation-related activities associated with onboarding and baseline assessment. However, respondents should also account for the required ongoing annual penetration testing throughout the contract term and clearly identify how those costs will be billed.

For evaluation purposes, WCCAC seeks transparency regarding all recurring and periodic costs associated with performance of the contract.

7. HIPAA Security Program, PHI/PII, Access Controls, and Compliance

Question 50

Has the organization conducted a HIPAA assessment within the past twelve months? If so, are those findings available to the winning firm? Yes, our HIPAA Risk Assessment was completed in April 2026. It will be made available after contract completion.

Question 51

Are data flows currently mapped end to end that contain PHI (patient intake to archival)? WCCAC has not yet confirmed whether comprehensive end-to-end PHI/ePHI data-flow documentation is currently maintained. Certain information, including case management information, is maintained in systems provided through statewide or other third-party organizations, while medical information may be maintained through separate systems or processes. Access to PHI and other sensitive information is role-based, with personnel provided only the minimum level of access necessary for their assigned responsibilities.

As part of the discovery and transition process, the selected provider will be expected to review available documentation, validate existing PHI/ePHI data flows, identify any documentation gaps, and assist WCCAC in developing or updating the necessary data-flow documentation as part of the HIPAA security assessment.

Question 52

What access controls are currently in place? WCCAC utilizes role-based access controls and follows a minimum-necessary approach, with users provided access based on their assigned job responsibilities. Physical and logical access to systems, networks, applications, and sensitive information is restricted to authorized personnel. Additional controls are applied to secure areas and sensitive systems.
Existing access controls, account permissions, administrative access, and related security configurations will be validated during the selected vendor's discovery and security assessment. Respondents should identify any additional access-control capabilities or recommendations included in their proposed solution.

Question 53

What encryption standards are in place for data in transit and data at rest? WCCAC utilizes security and encryption capabilities provided through its existing systems and cloud services; however, specific encryption standards and configurations have not been independently validated for purposes of this solicitation.
The selected provider will be expected to review and validate encryption protections for sensitive data in transit and at rest during the discovery and security assessment and identify any gaps or recommended improvements. Respondents should describe the encryption standards and controls included in their proposed solution and identify any assumptions, licensing requirements, or recommended changes necessary to meet applicable security and HIPAA requirements.

Question 54

Is there a current vendor risk management lifecycle in place? WCCAC currently performs vendor oversight through contracting, confidentiality and security requirements, access controls, insurance requirements, screening and training requirements, and Business Associate Agreements where applicable. WCCAC is continuing to formalize its overall vendor risk management lifecycle, including risk assessment, ongoing monitoring, periodic review, and offboarding. The selected provider may be asked to assist WCCAC with strengthening and documenting this process as part of the HIPAA Security Program.

Question 55

Does WCCAC already have a HIPAA Security Risk Analysis, approved security policies, POA&M, and a compliance-management platform? Would WCCAC permit the selected provider to use its own compliance platform to manage the program and provide WCCAC-accessible reporting/exports? WCCAC has an approved Risk Analysis, policies, and POA&M that will be made available during discovery. We would permit the MSP to have their own platform.

Question 56

Are there geographic, citizenship, residency, or U.S.-person restrictions for remote personnel or subcontractors accessing WCCAC systems, including any CJIS-connected systems? Please identify requirements by system or role. While not a mandatory requirement, WCCAC prefers U.S.-based personnel for administrative access to systems containing sensitive or regulated information and may consider staffing location as part of its overall best-value evaluation.

Question 57

For annual HIPAA awareness/role-based training and the required tabletop exercise, does WCCAC expect onsite facilitation? Approximately how many participants and what roles should be included? We are open to remote training. The tabletop exercises involve our leadership team of about 12 -14 persons.

Question 58

Are there any regulatory, audit, or internal requirements governing vulnerability remediation timelines? WCCAC expects vulnerability management to follow a risk-based approach, with identified vulnerabilities prioritized based on severity, exploitability, exposure, and operational impact. Vulnerability findings may also be incorporated into WCCAC's HIPAA risk assessment and remediation/POA&M process, as applicable. Respondents should describe their recommended remediation timelines, escalation procedures, and process for tracking findings through remediation or documented risk acceptance.

Question 59

For annual penetration testing, should testing cover: Yes, Internal infrastructure, External infrastructure, Web applications, Microsoft 365 environment, Wireless networks

Question 60

May respondents propose written exceptions or revisions to the draft Business Associate Agreement's breach-related cost provisions through Attachment J? As noted in the RFP, respondents may submit requested exceptions to the Business Associate Agreement with their proposal. Any proposed exceptions, revisions, or alternative language should be clearly identified and explained for WCCAC's review and consideration during the evaluation and negotiation process.

Question 61

Which line-of-business systems hold PHI or criminal justice information (case management, forensic interview recordings, shared drives, on-premises servers), and are they cloud-hosted or on-site? We have several systems that are cloud-based that hold PHI,PII such as case management, shared drives, etc. Our forensic interview systems have on-premise servers, and our medical system relies on cloud base and NAS. WCCAC does not maintain a CJIS system of record. However, WCCAC personnel may access information received from law enforcement and multidisciplinary partners in the course of providing services to children and families.

WCCAC's internet connectivity is provided through Williamson County, and network access is protected through county-managed security controls, including firewall protections. In addition, WCCAC's server room is subject to CJIS-related physical security requirements. As a result, vendor personnel requiring unescorted physical access to the server room may be required to satisfy applicable CJIS access requirements in effect at the time access is requested.

Question 62

For personnel screening, can background checks and SafeSport, CJIS, and HIPAA training be completed for our named staff between award and the November 2 start, or must they be on file before award? The personnel screening can be completed between award and contract start date and before any on-site access.

Question 63

Part VII, subcontractor screening. Do the criminal background, sex offender registry, SafeSport, and CJIS training requirements apply to subcontractor personnel who work only with security monitoring data and have no interactive access to WCCAC systems or PHI? If they do apply, will WCCAC accept a written

attestation from the subcontractor in place of individual evidence? The background requirements are for those who have physical access to our systems.

8. Applications, SaaS, Vendors, Subcontractors, Personnel, and CJIS

Question 64

What is your Electronic Medical Record or Case Management System? Is it hosted? We utilize 3rd party systems for Case Management that is provided by our state organization. It is cloud based. Our medical system is cloud based as well, although we utilize one NAS: Synology for specialized medical.

Question 65

Are there physical or virtual servers, NAS devices, cloud-hosted servers (including Azure), or other infrastructure not reflected in the inventory? If none, can WCCAC confirm that applications and data are primarily SaaS-based?

WCCAC is mostly virtual using Microsoft 365. We do have one NAS: Synology for specialized medical and 2 physical servers for our forensic interview system. Both the medical and forensic interview system are managed by WCCAC with assistance from our MSP for technical issues. Both are on service contracts and we anticipate some MSP assistance on these services for system updates.

Question 66

What core SaaS and business applications require support, including case management, forensic interview/recording, finance, and partner-facing systems? What is the support responsibility of each application vendor? WCCAC utilizes several SaaS and business applications supporting case management, forensic interview/recording, finance, administrative functions, and partner-facing activities. Specific application details will be reviewed with the selected vendor during discovery and onboarding.

In general, the individual application vendors are responsible for application-specific functionality, hosting, maintenance, and vendor-supported updates. WCCAC communicates and coordinates with its software vendors regarding application updates and changes, but relies on its MSP for the technical assistance necessary to implement or support those changes within the WCCAC environment.

The selected MSP will be expected to assist with user access, accounts, device configuration, connectivity, troubleshooting, installation or deployment of updates where applicable, and coordination with WCCAC and the application vendor when technical issues require escalation.

Respondents should describe their approach to supporting third-party SaaS and business applications and coordinating with WCCAC and application vendors.

9. Governance, Service Levels, Pricing, Insurance, and Contract Terms

Question 67

Are there any personal devices for staff or volunteers that require management and/or support? No

Question 68

What is your annual budget for IT services? WCCAC has not established a fixed budget for this solicitation. As a nonprofit organization, WCCAC has a responsibility to be fiscally responsible while ensuring that its technology, cybersecurity, and compliance needs are appropriately supported.

We recognize that the amount for our current contract scope and quantities does differ from the RFP as we have seen an increase in growth/devices.

Respondents should propose pricing based on the requirements of the RFP and clearly identify the services included, associated costs, assumptions, exclusions, and overall value. WCCAC is seeking a solution that provides the appropriate level of service, security, compliance support, and responsiveness at a reasonable and sustainable cost for a nonprofit organization.

Proposals will be evaluated on overall best value rather than solely on lowest price.

Question 69

Of the 75–85 workstations/laptops, what is the approximate Windows/Mac split, and are any personally owned? All of our laptops are Dell (various models), with the exception of one (MAC) in use and 5 mini-PCs (Beelink).

Question 70

Should vulnerabilities, unsupported systems, or technology gaps identified during initial discovery be presented as separately approved remediation projects rather than included in the recurring fixed fee? Vulnerabilities, unsupported systems, and technology gaps identified during discovery should be documented, prioritized, and presented to WCCAC with recommended remediation actions. Routine remediation that falls within the scope of the recurring managed services should be included in the fixed fee.

Items requiring significant hardware or software purchases, major upgrades, replacements, or project-based work outside the recurring scope should be separately identified, priced, and submitted to WCCAC for approval before work is performed.

Respondents should clearly identify in their proposal what remediation activities are included in the recurring fee and what types of work would be treated as separately approved projects.

Question 71

Can you provide a current network diagram and high-level architecture documentation? We will be able to provide this during discovery phase.

Question 72

Does WCCAC expect a dedicated technical account manager, vCIO, security advisor, or governance lead as part of ongoing support? WCCAC expects the selected provider to provide appropriate account management, strategic technology guidance, security oversight, and governance support as part of the ongoing relationship. These functions do not need to be provided by separate dedicated individuals.

Respondents should describe their proposed account management and governance structure, including the roles responsible for service oversight, technology strategy, cybersecurity, HIPAA security support, reporting, and escalation.

Question 73

Can you confirm the required SLA measurements, reporting metrics, and service review expectations? Yes. The required SLA measurements, reporting metrics, and service review expectations are outlined in Part VIII and Attachment E of the RFP. Respondents should address the stated response-time requirements and propose restoration and resolution targets, escalation thresholds, and service-hour definitions.

WCCAC expects monthly service and security reporting, quarterly executive/technical reviews, vulnerability reporting, and Quarterly Business Reviews (QBRs). Respondents may propose additional metrics or reporting they believe would provide value to WCCAC.

Question 74

Are quarterly business reviews mandatory, and what information should be included within those reviews? Yes. Quarterly Business Reviews (QBRs) are expected as part of the ongoing services.

QBRs should provide an executive-level review of service performance, cybersecurity and vulnerability trends, HIPAA/security program status, significant risks, technology lifecycle and roadmap items, projects, budget considerations, and recommendations or decisions requiring WCCAC attention.

Respondents may include additional information they believe would be valuable to WCCAC.

Question 75

Is the intent of this procurement primarily managed services, or is the selected provider also expected to supply software licensing as part of the engagement? Primarily manages services.

Question 76

Are there any known operational, cybersecurity, compliance, staffing, or technology challenges that WCCAC would like the selected provider to prioritize during the initial contract period? We do anticipate towards the end of the contract period a possible change in our forensic interview system.

Question 77

Insurance: Must all certificates accompany the proposal, or may a selected vendor provide them before contract execution? For a founder-operated company, would legally applicable workers' compensation exemptions and hired/non-owned automobile liability coverage be considered? The selected vendor will be required to provide evidence of the required insurance coverage prior to contract execution, but not at the time of the proposal.

Respondents should identify any exceptions, limitations, or alternative coverage arrangements in their proposal for WCCAC's review. WCCAC will consider legally applicable workers' compensation exemptions and hired/non-owned automobile liability coverage, where appropriate, provided the respondent clearly explains the proposed coverage and demonstrates that the intent of the insurance requirements is satisfied.

WCCAC reserves the right to review and approve all insurance documentation prior to contract award and execution.

Question 78

Term and pricing. Should pricing for the two optional renewal years be included now, and may Attachment A show one bundled monthly price with an allocation across the A3 lines? Yes. Respondents should include pricing for any proposed renewal terms with their response. Pricing for the initial term and each optional renewal

year should be clearly identified, including any annual increases, pricing adjustments, assumptions, or escalators that may apply.

Regarding Attachment A, respondents may provide a bundled monthly service fee provided that the pricing structure is transparent. The bundled amount should be allocated across the applicable A3 line items, or accompanied by a narrative that clearly identifies how the bundled services map to the requested service categories.

WCCAC's objective is to understand both the total cost of ownership and the relative cost of the major service components being proposed. Respondents should provide sufficient detail to allow WCCAC to evaluate pricing, compare proposals, and understand any included services, exclusions, assumptions, optional services, and recurring costs.

Question 79

Evaluation. How will the 10 pricing points be scored: lowest price, a formula, or overall value? Pricing will be evaluated on a best-value basis rather than solely on lowest cost. The Pricing and Overall Value score will consider the competitiveness, completeness, transparency, and overall value of the proposed pricing in relation to the services offered.

A lower-priced proposal will not automatically receive the highest score, and WCCAC reserves the right to select the proposal that provides the best overall value to the organization.