VILLAGE OF WESTCHESTER

Cook County, Illinois

ADDENDUM NO. 2

Vendor Questions and Village Responses

RFQ:	Managed Cybersecurity Detection, Response, and Monitoring Services
RFQ Number:	RFQ-2026-009
Addendum Issued:	June 17, 2026
Submitting Firms:	Multiple Respondents
Status:	**ISSUED**

This Addendum responds to written questions received from prospective Respondents during the Question and Answer period. The information contained herein is incorporated into and made part of the RFQ. Respondents shall acknowledge receipt of this Addendum in their cover letter as required by Section 4.3 of the RFQ. Where a question has been previously addressed in Addendum No. 1, this Addendum directs Respondents to the prior response rather than restating it. ***Respondents are reminded that all previously issued Addenda are part of the RFQ and shall be reviewed in full prior to submission of a final Quotation. Thoroughness in the review of solicitation materials may be considered as a factor in evaluation under RFQ Section 6.***

Notice: This Addendum constitutes the Village's final response to written inquiries. Effective upon issuance of this Addendum, the Question and Answer period for RFQ-2026-009 is closed. No further questions will be received, considered, or responded to. Respondents shall prepare and submit their Quotations on the basis of the RFQ as amended by Addendum No. 1 and this Addendum No. 2.

1. Service Model and Roles

Question 1

> *Please clarify the expected division of responsibilities between the Village's internal IT staff and the selected Vendor, particularly with respect to day-to-day security operations.*

RESPONSE

The Village operates with a single in house Senior Technology Officer who retains ownership of asset inventory, identity provisioning, change management, and final approval authority for actions outside agreed playbooks. The selected Vendor shall own all day to day security operations including continuous monitoring, alert triage, investigation, threat hunting, and standard containment actions executed under pre agreed playbooks. The Vendor SOC functions as an extension of the Village's IT function rather than as a tier of escalation that gates Village response. Vendor analysts shall not require per incident approval to execute routine containment within scope.

Question 2

> *Will the Vendor be expected to act as the primary authority for cybersecurity operations, or will all actions require prior approval from Village personnel?*

RESPONSE

The Vendor shall act as the primary operational authority for cybersecurity detection and response within the scope of pre agreed playbooks. Actions outside playbook scope, including but not limited to wide scale identity revocation, server takedown, public communications, and law enforcement engagement, require Village approval through a documented escalation matrix. Respondents shall describe their model for balancing decisive autonomous response with appropriate Village oversight, and how they handle after hours decision making when Village personnel may not be immediately reachable.

Question 3

> *Are there existing managed service providers or third-party IT partners currently supporting the environment? If so, how will responsibilities be coordinated across organizations?*

RESPONSE

The Village does not currently engage a general purpose managed service provider for IT operations. Custom application development and infrastructure operations are performed in house by the Senior Technology Officer. The selected Vendor will coordinate directly with the Senior Technology Officer for all matters. No coordination with a separate MSP is required.

Question 4

> *To what extent is the Vendor expected to define or influence security architecture versus operating within the Village's existing architecture?*

RESPONSE

The Vendor shall operate within the Village's existing architecture. The Vendor is expected and encouraged to make recommendations for architecture changes that materially improve security posture,

particularly during quarterly strategic reviews. Implementation of any architecture change is performed by Village staff with Vendor consultation. The Vendor is not authorized to alter the Village's network, identity, or application architecture unilaterally.

2. Security Tooling and Platform Expectations

Question 5

> *Is the Village seeking a fully consolidated, Vendor-provided cybersecurity platform, or should proposals assume integration with existing tools?*

RESPONSE

The Village prefers a consolidated Vendor provided platform that integrates natively with Microsoft 365, Microsoft Entra ID, Ubiquiti network infrastructure, and Mosyle Mobile Device Management. The Village is not seeking a best of breed multi vendor stack assembled by the Respondent. Respondents shall describe their platform consolidation philosophy and the depth of native integration they offer with the systems identified above.

Question 6

> *Please identify any incumbent security technologies (e.g., endpoint protection, SIEM, email security) that must be retained as part of the solution.*

RESPONSE

The following technologies are retained as part of the Village environment and shall continue to operate alongside the Vendor solution: Microsoft Defender for Endpoint and Microsoft Defender for Office 365 (where licensed by Microsoft 365 G3 entitlement), and the Village's custom built email security platform ("WASP"). The Village's current managed security service is provided by Huntress and includes Managed EDR, Managed ITDR, and Managed SIEM. The Village has not made a final determination regarding the incumbent managed service and will evaluate Quotations on their merits. Respondents shall describe how their platform interoperates with Microsoft Defender telemetry and shall not require removal of Defender as a condition of deployment.

Question 7

> *If replacement of existing tools is permitted, should Vendors include transition and licensing optimization considerations in their proposals?*

RESPONSE

Yes. Respondents are encouraged to identify opportunities for transition simplification and licensing optimization in their proposals. Any such optimization shall be clearly documented and presented as optional unless required by the proposed solution.

Question 8

> *Given the Village's Microsoft 365 GCC G3 environment, should Vendors assume utilization of Microsoft-native security capabilities, or propose alternative solutions?*

RESPONSE

Respondents should leverage Microsoft 365 native security capabilities where they provide value, including Defender for Office 365, Audit (Premium) telemetry for G3 licensed identities, and Entra ID sign in logs. As clarified in Addendum No. 1, the Village's tenant is a mixed Microsoft 365 Government

Community Cloud environment with 115 G1 licenses and 11 G3 licenses, not a pure G3 tenant. Respondents shall not assume Defender for Office 365 telemetry is available for G1 licensed identities and shall describe how their platform compensates for the reduced telemetry available from G1 accounts.

3. Incident Response Authority and Procedures

Question 9

> *Please clarify the level of authorization that may be granted to the Vendor for containment actions such as endpoint isolation, account disablement, and session revocation.*

RESPONSE

Vendor SOC analysts shall be authorized to perform the following containment actions under pre agreed playbooks without per incident Village approval: endpoint host isolation, user account disablement, active session revocation, blocking of malicious sender domains, deletion of malicious mail items from user mailboxes, and quarantine of malicious files. The Vendor shall provide real time notification to the Village of every containment action taken, including the rationale and indicators of compromise that justified it.

Question 10

> *Are there defined approval workflows for high-impact response actions, or may the Vendor act autonomously under agreed-upon playbooks?*

RESPONSE

Routine containment actions identified in Question 9 may be executed autonomously under playbook authority. High impact actions including but not limited to disablement of more than five (5) user accounts simultaneously, isolation of any domain controller or other Tier 0 asset, takedown of any production server, communications to staff or the public, and engagement with law enforcement, require Village approval via the documented escalation matrix prior to execution.

Question 11

> *Are there special restrictions or procedures for systems subject to CJIS requirements, particularly within Police and Fire operations?*

RESPONSE

Yes. Systems subject to CJIS Security Policy, including those processing or storing Criminal Justice Information (CJI), are subject to additional controls. Vendor personnel with logical or physical access to such systems shall complete CJIS Security Awareness training and a fingerprint based background investigation through an Illinois LEADS certified entity prior to access. The Vendor shall execute a CJIS Security Addendum and shall ensure all data storage and transmission related to in scope systems complies with the current CJIS Security Policy.

Question 12

> *What escalation and communication expectations apply during active incidents, including required availability of Village personnel?*

RESPONSE

The Vendor shall maintain a documented escalation matrix listing primary, secondary, and after hours contacts for the Village. During active incidents the Village shall make a designated representative available within the following windows: critical severity (60 minutes), high severity (4 hours), medium and

low severity (next business day). The Vendor shall provide a dedicated incident bridge or secure messaging channel for use during major incidents.

Question 13

> *Does the Village currently maintain an incident response retainer or external partner, and if so, how should coordination be handled?*

RESPONSE

The Village does not currently maintain a separate dedicated incident response retainer with an external partner. Respondents shall describe the incident response coverage included in base pricing under the resulting contract and shall identify any optional incident response retainer add ons available. In the event the Village engages a separate digital forensics or breach counsel firm in response to a specific incident, the awarded Vendor shall cooperate with that firm under Village direction.

4. SIEM Scope, Data Ingestion, and Retention

Question 14

> *Can the Village provide estimated daily or monthly log ingestion volumes by source to assist with accurate sizing and pricing?*

RESPONSE

Aggregate ingest data is provided in Addendum No. 1, Question 1. The Village's current Managed SIEM (Huntress) reports approximately 6 GB per day of stored and indexed data, and approximately 15 to 20 GB per day of pre filter collection, based on the May 2026 baseline. Per source ingest breakdowns are not separately metered in the current platform. Respondents shall scope sizing based on the asset and log source inventory provided in RFQ Section 2.3 and the aggregate ingest figure above.

Question 15

> *Should all listed log sources be assumed in scope for initial onboarding, or may Vendors propose phased ingestion?*

RESPONSE

Phased ingestion is acceptable. Respondents shall propose a phasing plan that prioritizes the following sources in Phase 1, to be onboarded within thirty (30) days of contract execution: Microsoft 365 and Entra ID, on premises Active Directory, the Ubiquiti edge firewall, and EDR agent telemetry. Remaining log sources shall be onboarded within ninety (90) days of contract execution. Respondents shall identify any source they consider impractical for ingestion and the reasoning.

Question 16

> *Are any data sources considered optional or out of scope for the initial deployment?*

RESPONSE

Mobile device telemetry from Mosyle Mobile Device Management is considered optional in Phase 1 if its inclusion materially affects pricing. The Village's preference is for inclusion if cost neutral. All other sources listed in RFQ Section 2.3 are in scope.

Question 17

> *For extended log retention beyond the required period, please clarify expected retention levels and access requirements.*

RESPONSE

Retention requirements are defined in RFQ Section 2.3: three hundred sixty five (365) days of hot, searchable retention and twenty four (24) months of cold or archive retention available on request. The Village does not currently require retention beyond this baseline. Respondents shall describe per gigabyte or per event archive retrieval pricing if applicable.

Question 18

> *Are there any preferred or pre-existing SIEM platforms that Vendors should consider in their proposals?*

RESPONSE

The Village has no preferred SIEM platform and will evaluate all responsive Quotations on the basis of capability, fit, and total cost. Respondents shall propose their own SIEM solution as a standalone offering and shall not assume integration with or continuation of the incumbent platform.

5. Environment and Asset Details

Question 19

> *Please provide an approximate breakdown of endpoint types (e.g., servers, user workstations, macOS systems).*

RESPONSE

Endpoint breakdown is provided in Addendum No. 1, Question 6. Current EDR agent deployment: seventy one (71) Windows 10 / 11 workstations, six (6) Windows Server 2019 / 2022 instances, zero (0) macOS devices. In addition, ten (10) Linux server instances are hosted in cloud infrastructure without a current EDR agent and shall be in scope for SIEM log ingestion. Thirty five (35) mobile devices are managed by Mosyle Mobile Device Management.

Question 20

> *Are any systems segmented, air-gapped, or otherwise restricted from standard monitoring or response actions?*

RESPONSE

The Village's primary network is flat at the routing layer but uses VLAN segmentation for the Police Department subnet, the Fire Department subnet, and the Public Works / SCADA subnet. No system is currently air gapped. Police Department endpoints handling Criminal Justice Information are reachable for monitoring but containment actions on those endpoints shall be performed only under coordination with the Police Department per the CJIS provisions described in Section 3.

Question 21

> *What level of administrative access will be granted to the Vendor for monitoring and response activities?*

RESPONSE

The Vendor shall be granted scoped service account access sufficient to perform the contracted services. Specifically: read access to Microsoft 365 unified audit log, Entra ID sign in logs, and Defender telemetry; read access to on premises Active Directory; read access to firewall and switch syslog; agent installation and response action authority on managed endpoints. Domain Administrator and Global Administrator level access will not be granted on a standing basis. Time bounded elevated access may be granted during a confirmed incident under Village approval.

Question 22

> *Should mobile devices be considered in scope for full threat detection and response, or limited to management telemetry?*

RESPONSE

Mobile devices are in scope for management telemetry from Mosyle Mobile Device Management, including compliance state, application inventory, and indicators of jailbreak or root. Full mobile threat defense (MTD) such as on device behavioral monitoring is not required in base scope. Respondents may

include MTD capability as an optional line item and shall describe what their platform provides for mobile device threat detection.

Question 23

> *Please provide additional context regarding workloads hosted in Vultr and protected by Cloudflare.*

RESPONSE

The Village operates ten (10) Linux server instances hosted on Vultr supporting custom municipal applications and services, including but not limited to meeting management, document management, ticketing and asset management, email security, and resident facing services. Cloudflare provides edge security including DDoS mitigation, web application firewall, and TLS termination for public facing endpoints. Respondents shall describe their capability to ingest Cloudflare logs (Cloudflare Logpush or comparable mechanism) and their support for monitoring Linux server endpoints, including whether a Linux EDR agent is included in base pricing.

6. Service Levels and Performance Measurement

Question 24

> *How will service level performance (e.g., time to detect, triage, and escalate) be measured and validated?*

RESPONSE

Service level performance shall be measured by the Vendor and reported monthly in the executive summary report described in RFQ Section 2.6. The Village reserves the right to audit SLA performance through review of incident timestamps, ticket data, and supporting evidence. Respondents shall describe the specific timestamps and event records they use to compute time to detect, time to triage, and time to escalate metrics.

Question 25

> *Does SLA timing begin at the point of event occurrence, detection, or ingestion into the monitoring platform?*

RESPONSE

SLA timing begins at the point of log ingestion into the Vendor monitoring platform. SLA timing does not include transmission delay from the Village endpoint or log source to the Vendor platform, provided the Vendor confirms ingestion health monitoring is in place to detect interrupted feeds.

Question 26

> *How are false positives treated in the context of SLA performance metrics?*

RESPONSE

False positives correctly triaged and dismissed by the Vendor SOC do not count against SLA performance. False positives escalated to the Village without sufficient triage shall be tracked separately and reported monthly. A pattern of low quality escalations may be treated as a service performance issue and addressed through service credits or contract remediation.

Question 27

> *Please provide additional detail regarding service credit structures tied to SLA performance.*

RESPONSE

Service credits will be defined in the resulting contract. The Village's initial framework is a five percent (5%) credit against the monthly recurring fee for each SLA category missed in a given month, cumulative up to a maximum of twenty five percent (25%) of the monthly recurring fee in any single month. Service credits are the Village's exclusive remedy for individual SLA misses; the Village's right to terminate for material breach under RFQ Section 7.3 remains unaffected.

7. Reporting and Governance

Question 28

> *Who are the primary stakeholders for monthly and quarterly reporting (e.g., technical staff, executive leadership, governing board)?*

RESPONSE

Primary monthly reporting recipients are the Senior Technology Officer and the Village Manager. The quarterly executive summary report shall also be distributed to the Village President and the Village Board of Trustees in summary form, excluding any content subject to CJIS Security Policy restrictions or exempt from public disclosure under the Illinois Freedom of Information Act. Police and Fire Chiefs receive incident reporting that pertains to their respective departments.

Question 29

> *What level of detail and analysis is expected in quarterly strategic reviews?*

RESPONSE

Quarterly strategic reviews shall include, at minimum: detection trend analysis for the quarter, threat landscape briefing relevant to the municipal sector, gap analysis against current Village security posture, prioritized recommendations for posture improvement, summary of significant incidents and their root cause findings, and review of SLA performance for the quarter. Reviews shall be conducted via video conference with a dedicated account contact and supplemented by a written report.

Question 30

> *Are there specific compliance or regulatory reporting requirements beyond those outlined in the RFP?*

RESPONSE

In addition to internal Village reporting, the Vendor shall be capable of supporting the following: Illinois Personal Information Protection Act (815 ILCS 530) breach notification documentation, CJIS annual audit response, Illinois Local Records Act retention compliance, and Illinois Freedom of Information Act compatible reporting (with appropriate redaction of CJI and exempt material). The Vendor is not required to be the system of record for these reports but shall supply data on request in usable formats.

Question 31

> *Are integrations with existing reporting tools or dashboards required?*

RESPONSE

Direct integration with existing Village reporting tools is not required at contract commencement. The Vendor portal as described in RFQ Section 2.6 shall serve as the primary interface. API access to detection and incident data is required to support potential future integration with Village dashboards. Respondents shall describe the API capabilities of their platform.

8. Compliance and CJIS Requirements

Question 32

> *Please clarify which systems and data sets fall within CJIS scope.*

RESPONSE

Systems within CJIS scope include all Police Department workstations and servers, mobile data terminals deployed in police vehicles, body worn camera storage and management systems, dispatch related systems, and any system processing or storing Criminal Justice Information including but not limited to NCIC and Illinois LEADS interface data. Fire Department systems that process CJI in the course of EMS or investigative work are also within scope. The Village's identity infrastructure (Active Directory and Entra ID) is in scope to the extent it authenticates access to CJI systems.

Question 33

> *Are CJIS-specific background investigations (e.g., fingerprint-based checks) required for Vendor personnel?*

RESPONSE

Yes. Vendor personnel with logical or physical access to CJI systems must complete fingerprint based background investigation through an Illinois LEADS certified entity prior to access being granted, and shall complete CJIS Security Awareness Training (level four) on the same timeline. The cost of background investigations is the responsibility of the Vendor. The Village will facilitate the fingerprinting process through coordination with the Police Department.

Question 34

> *Are there existing CJIS audit findings or remediation priorities that Vendors should address?*

RESPONSE

The Village has no open CJIS audit findings at this time that require Vendor remediation. Respondents shall be prepared to support remediation of any future findings identified during the audit cycle and shall describe their experience supporting municipal customers through CJIS audits.

Question 35

> *Are there additional CJIS-related requirements beyond those referenced in the RFP that Vendors should anticipate?*

RESPONSE

Respondents shall anticipate the following beyond the requirements stated in RFQ Section 3.1: execution of a CJIS Security Addendum prior to access; maintenance of personnel screening documentation made available on Village request; quarterly attestation of continued personnel compliance; and compliance with the encryption, access control, audit, and incident response provisions of the current CJIS Security Policy. The Village will provide the Vendor with the current Policy version applicable at the time of contract execution.

9. Pricing and Commercial Structure

Question 36

> *Please confirm the approximate number of user identities for pricing purposes.*

RESPONSE

Identity count is provided in Addendum No. 1, Question 5. The Village has one hundred twenty six (126) total licensed identities consisting of one hundred fifteen (115) Microsoft 365 G1 and eleven (11) Microsoft 365 G3 licenses. Respondents shall price for the full 126 identities under Identity Threat Detection and Response.

Question 37

> *Is there an anticipated budget range or target cost model for this engagement?*

RESPONSE

The Village's position on budget is provided in Addendum No. 1, Question 7. No fixed not to exceed budget has been established. Quotations will be evaluated on best value in accordance with the weighted criteria in RFQ Section 6.

Question 38

> *How many incident response hours are expected to be included annually?*

RESPONSE

Respondents shall include in base annual pricing a minimum of forty (40) hours of dedicated incident response support per contract year, inclusive of analyst time, forensic triage, and post incident reporting. Additional incident response hours shall be available at a clearly stated hourly rate. The Village will not pre commit to a specific volume of additional hours.

Question 39

> *Should Vendors assume growth in endpoints, users, or log volume over the contract term, and if so, at what approximate rate?*

RESPONSE

Respondents shall assume modest organic growth of approximately five percent (5%) to ten percent (10%) per contract year in endpoints, identities, and log ingest. Pricing shall accommodate this growth without renegotiation. Material expansion outside this range, such as the addition of a new department, facility, or substantial new technology footprint, shall be addressed by contract amendment.

10. Implementation and Transition

Question 40

> *Is there an incumbent Vendor or solution currently in place that will be transitioned out?*

RESPONSE

Huntress is currently in place providing Managed Endpoint Detection and Response, Managed Identity Threat Detection and Response, and Managed Security Information and Event Management. The Village has not made a final determination regarding transition of the incumbent solution. Respondents shall describe their transition methodology assuming a full replacement scenario, and may also describe coexistence or hybrid approaches as alternatives where applicable. Continuous monitoring coverage during any transition period is required and shall be addressed in the Respondent's implementation plan.

Question 41

> *What is the desired timeline for implementation and transition to steady-state operations?*

RESPONSE

The Village's target is ninety (90) days from contract execution to full steady state operations, with Phase 1 critical source ingestion and EDR agent rollout completed within the first thirty (30) days. Respondents may propose alternative timelines if supported by methodology and resourcing. Faster implementations will be viewed favorably provided they do not compromise quality or stability.

Question 42

> *Are there constraints on deployment scheduling, particularly for public safety or critical systems?*

RESPONSE

Yes. Deployment activity affecting Police Department or Fire Department endpoints, dispatch systems, body worn camera infrastructure, or Public Works SCADA shall be coordinated with the relevant Department head and may require execution outside of normal business hours. Maintenance windows for public safety systems are typically available overnight on weekdays or during early morning hours on weekends.

Question 43

> *What level of project management and internal resource support will be provided by the Village during implementation?*

RESPONSE

The Village will designate the Senior Technology Officer as the single point of contact for implementation and ongoing operations. The Village does not have a dedicated project manager available for vendor projects. Subject matter experts from Police, Fire, and Public Works will be made available for scoped activities through coordination with the Senior Technology Officer. Respondents shall provide their own project management resource and shall not assume Village project management as part of the engagement.

11. References and Qualifications

Question 44

> *Will the Village accept references from outside the State of Illinois?*

RESPONSE

Respondents may submit references from outside the State of Illinois, however the requirement in Section 3.3 of the RFQ stands without amendment: a minimum of one (1) of the three (3) required customer references shall be from an Illinois municipal or other Illinois public sector customer. Respondents who fail to provide at least one (1) qualifying Illinois reference will be deemed non responsive.

12. Additional Vendor Inquiries

Question 45

> *What was the annual spend under the previous contract for these services? If this is a new contract, what is the estimated annual budget?*

RESPONSE

See Addendum No. 1, Question 7 and Question 37 of this Addendum. The Village has not established a fixed not to exceed budget for this procurement and will evaluate Quotations on the basis of best value in accordance with the weighted criteria in RFQ Section 6.

Question 46

> *Is the agency open to a hybrid delivery model utilizing a combination of onshore and offshore resources?*

RESPONSE

The Vendor's Security Operations Center may operate as an integrated team distributed across multiple locations, provided that all data storage and all analyst access to Village systems and data remain within the continental United States as required by RFQ Section 3.1. Pure offshore call center triage models will not be considered, consistent with RFQ Section 2.4. Respondents shall identify the geographic location of all SOC operations, all data storage, and all analyst personnel in their Quotation.

Question 47

> *Will the work be performed onsite, remotely, or through a hybrid arrangement?*

RESPONSE

The Vendor shall perform services remotely from its own facilities. Periodic onsite visits to the Village may be required for implementation kickoff, quarterly strategic reviews, or post incident debriefs at the Village's discretion. Routine SOC monitoring, triage, and response activity shall not require an onsite Vendor presence.

Question 48

> *Would it be possible to consider a 1–2 week extension to the proposal submission deadline?*

RESPONSE

No. The Quotation Due date for this RFQ is July 31, 2026 at 2:00 PM Central Time, as set forth on the cover and in Appendix A of the RFQ. The Village has determined that the period from the original RFQ issuance through July 31, 2026 provides reasonable preparation time and will not extend the submission deadline.

Question 49

> *Is this contract intended for a single vendor or for multiple vendors?*

RESPONSE

The Village contemplates a single award to a primary Vendor of record. The Village reserves the right under RFQ Section 9.1 to award by individual component or in the aggregate if doing so demonstrates better value to the Village.

Question 50

> *Who is the current or previous incumbent vendor for these services?*

RESPONSE

See Question 40 of this Addendum. Huntress currently provides Managed Endpoint Detection and Response, Managed Identity Threat Detection and Response, and Managed Security Information and Event Management to the Village.

Question 51

> *Are there any challenges, gaps, or pain points with the current solution or contractor that the agency is looking to address through this procurement?*

RESPONSE

The Village's objective in this procurement is to consolidate security capability and align managed service scope with the asset and identity inventory described in RFQ Sections 1.3 and 2.3. The Village is not seeking remediation of specific deficiencies in the current solution and will not provide commentary on incumbent performance. Respondents shall propose their solution on its merits, not in comparison to incumbent capabilities.

Question 52

> *Is there a projected contract award date and anticipated start date?*

RESPONSE

The Village's general schedule is described in Appendix A of the RFQ. Specific contract award and service commencement dates will depend on the final Quotation submission date and the Village's evaluation timeline. Successful Respondents shall be prepared to commence transition activities within thirty (30) days of contract execution.

END OF VILLAGE RESPONSES TO WRITTEN QUESTIONS. The Question and Answer period is closed. Respondents shall prepare their Quotations in accordance with the RFQ as amended by Addendum No. 1 and this Addendum No. 2.

— END OF ADDENDUM NO. 2 —