VILLAGE OF WESTCHESTER

Cook County, Illinois

ADDENDUM NO. 1

Vendor Questions and Village Responses

RFQ:	Managed Cybersecurity Detection, Response, and Monitoring Services
RFQ Number:	RFQ-2026-009
Addendum Issued:	June 5, 2026
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.

Vendor Questions and Village Responses

The following questions were submitted by prospective Respondents. The Village's responses follow each question. Where information remains to be supplied by the Village, the response indicates a placeholder that will be replaced by the time this Addendum is issued.

Question 1: Current Daily Data Ingestion

> *Do you know the current daily data ingested for the environment daily for the current MDR solution (GB/day)?*

RESPONSE

The Village currently operates Huntress Managed SIEM in addition to Managed EDR and Managed ITDR. Recent monthly stored ingest figures from the Huntress platform are as follows:

- February 2026: approximately 420 GB
- March 2026: approximately 365 GB
- April 2026: approximately 270 GB
- May 2026: approximately 185 GB

May 2026 represents the most stabilized month following ongoing tuning and Smart Filtering optimization. May figures equate to approximately 6 GB per day of stored and indexed data and approximately 15 to 20 GB per day of pre filter collection. The Village's current annual data pool allocation is 14,880 GB.

Respondents should scope ingest based on the May 2026 baseline. Respondents shall describe in their response whether their platform pricing is based on raw ingest volume, post filter stored volume, or both, and shall disclose any pre ingest noise reduction or filtering capability comparable to Smart Filtering.

Question 2: Alternative Security Attestation

> *Are you willing to accept CMMC Level 2 Certification (C3PAO Assessed) in addition to ISO 17020 Accreditation in lieu of SOC 2 Type II since it is equivalent or higher in terms of security/rigor?*

RESPONSE

Yes. Section 3.1 of the RFQ is hereby amended to read as follows:

> *"Vendor shall maintain a current SOC 2 Type II attestation; OR, in the alternative, a current CMMC Level 2 Certification assessed by an accredited C3PAO; OR a substantially equivalent independent third party security attestation acceptable to the Village in its sole discretion. The supporting report or certificate shall be made available to the Village under non disclosure agreement upon request."*

All other provisions of Section 3.1 remain unchanged.

Question 3: Number of Firewalls in Scope

> *What is the number of firewalls in scope for monitoring?*

RESPONSE

The Village operates one (1) edge firewall at its primary site. The firewall is a Ubiquiti Enterprise Fortress Gateway (EFG). All inbound and outbound traffic for the Village environment traverses this device. Respondents shall confirm that their platform supports ingestion of Ubiquiti firewall logs via syslog, and shall describe any parser or content pack specifically tuned for the Ubiquiti Unifi log format.

Question 4: Number of Switches in Scope

> *What is the number of switches in scope for monitoring?*

RESPONSE

The Village operates thirteen (13) managed network switches across its environment. All switches are manufactured by Ubiquiti Networks and are administered through a centralized Unifi controller. Respondents shall confirm support for ingesting Ubiquiti Unifi switch telemetry. The Village will determine on a case by case basis during implementation whether wireless access point logs are to be added as additional log sources beyond the switches; Respondents shall describe any incremental cost associated with adding wireless access point telemetry.

Question 5: Microsoft 365 / Entra ID Scope

> *Is Microsoft 365/Entra ID in scope for monitoring? If so, please provide the number of user accounts within AD/Entra ID to be monitored.*

RESPONSE

Yes, Microsoft 365 and Entra ID are in scope for monitoring under both the Identity Threat Detection and Response capability (Section 2.2) and the Security Information and Event Management capability (Section 2.3). The Village operates a hybrid Active Directory environment synchronized to Microsoft Entra ID within a Microsoft 365 Government Community Cloud tenant. The current licensed user breakdown is as follows:

License Type	Count
Microsoft 365 G1 (Government)	**115**
Microsoft 365 G3 (Government)	**11**

License Type	Count
TOTAL LICENSED IDENTITIES	**126**

Respondents should note that G3 licensed identities have access to richer audit and security telemetry sources, including Microsoft Defender for Office 365 and Audit (Premium), while G1 identities are limited to baseline Exchange Online and core directory telemetry. Respondents shall confirm that their Identity Threat Detection and Response capability functions across the full set of one hundred twenty six (126) identities regardless of underlying license tier, and shall identify any detection capability that is dependent on G3 or higher licensing. Pricing in the cost quotation shall be based on the full count of 126 identities unless otherwise clearly stated.

Question 6: Endpoint Breakdown

> *Can you provide a breakdown of the number of Windows Workstations vs. Servers vs. macOS devices so we can estimate ingest properly?*

RESPONSE

The Village currently has seventy seven (77) endpoint detection and response agents deployed across its environment. A breakdown by operating system is provided below.

Endpoint Type	Count
Windows Workstations (Windows 10 / 11)	**71**
Windows Servers (Server 2019 / 2022)	**6**
macOS Devices	**0**
TOTAL EDR AGENTS DEPLOYED	**77**

In addition to the endpoint agents listed above, the Village operates ten (10) Linux server instances hosted in cloud infrastructure that do not currently carry an EDR agent but will be in scope for SIEM log ingestion under any awarded contract. These instances host the Village's custom municipal applications and supporting services. The Village also operates approximately 35 mobile devices managed through Mosyle Mobile Device Management. Respondents shall indicate in their response whether their platform supports a Linux endpoint agent at no additional cost beyond the SIEM ingest fee, and whether mobile device telemetry from Mosyle is supported as a log source and included in base pricing or priced separately.

Question 7: Budget

> *Is there a budget available that the project must stay within?*

RESPONSE

The Village has not established a fixed not to exceed budget for this procurement. Quotations will be evaluated on best value in accordance with the weighted criteria set forth in Section 6 of the RFQ. The Village reserves the right to negotiate scope, pricing, and terms with any responsive Respondent.

— END OF ADDENDUM NO. 1 —