EL PASO COUNTY
COLORADO

El Paso County
Contracts and Procurement Division
15 East Vermijo Avenue
Colorado Springs, Colorado 80903

REQUEST FOR PROPOSAL RFP #25-007

Addendum #1 – January, 15, 2025

THIS ADDENDUM SHALL BECOME A PART OF THE SOLICITATION AND MUST BE ACKNOWLEDGED

Request for Proposal RFP-25-007 – Next Generation Information Security Operations Tools and Services - dated December 18, 2024

CLARIFICATIONS:

The deadline for submittals for this solicitation has been extended by one (1) week. Submittals will now be due by Wednesday January 29, 2025 at 1:00p.m. MST.

MULTIPLE VENDOR AWARD: The County may award to one or more vendors that are deemed to be in the best interest of El Paso County for the Next Generation Information Security Operations Tools and Services. The decision to award more than one vendor is a County prerogative and not a guarantee.

The County shall select those Vendors deemed to be most highly qualified to perform the required professional services after considering, and based upon, such factors as the ability of professional personnel, past performance, willingness to meet time and budget requirements, as well as current and projected workloads.

El Paso County will only accept electronic bid proposals submitted through the Rocky Mountain E-Purchasing system. A Submittal Log will be posted after the County has had an opportunity to review and verify the submittals offered to the County.

The original Offer must be received before the due date and time through an electronic package transmitted through the Rocky Mountain E-Purchasing system. The Vendor is responsible for ensuring its Response is posted in its entirety by the due date and time outlined in the solicitation document. No allowances will be provided to those Vendors whose submittal is not uploaded prior to the due date and time outlined in the solicitation.

If the submittal arrives late and/or is not uploaded in its entirety, it will not be included in the electronic lockbox.

ADMINISTRATION:

- The question period has expired
- Responses should follow the Response Format on pages 13 and include all responses to all mandatory requirements.
- We will be verifying submittals include the following:
    - Submittal properly acknowledged (Cover Sheet)
    - Addendum acknowledged
    - Evaluation Criteria Documentation
    - Exhibits 1-4
    - Vendor Information Form

- Proprietary/Confidential Statement
- Submission Form
- Completed W9

If a submittal is missing any of the above-mentioned documentation the submittal may be returned to the vendor as non-responsive and be deemed ineligible to participate.

RESPONSE TO QUESTIONS:

1.) Dear Cody Walters, We have the following questions What end points are you currently securing with Microsoft defender today? Would you consider changing those out to another solution following this solicitation? Do you want management of end points or end points and third party logs? Do you have an estimated ingest per day and logs per second count? Are your hot and cold storage requirements for incidents and or all logs? How do you collect telemetry from your networking devices today? Do you require cloud detection and response capabilities for AWS? Do you have other technologies/ work flows you'd like to automate with SOAR? Thank you for your consideration!

1a.) What end points are you currently securing with Microsoft defender today? We are not currently using defender to secure any endpoints (e.g., for EDR or web filtering). We are currently using Palo Alto Cortex XDR.

1b.) Would you consider changing those out to another solution following this solicitation? While we are currently happy with Cortex XDR performance and are not eager to switch at this time, we are open to having new EDR solutions included as an option in any proposal. Vendors proposing a different EDR solution must provide a comprehensive proposal that includes:
•Cost Transparency: All associated costs must be detailed, including professional services for initial deployment, configuration, and ongoing support.

•Justification for Alternative: A clear articulation of why their proposed EDR tool is a superior option compared to Cortex XDR, supported by objective data such as performance metrics, independent evaluations, or case studies. This approach ensures we can make an informed decision based on both cost-effectiveness and the ability to meet our operational and security requirements.

1c.) Do you want management of end points or end points and third-party logs? Our organization requires a comprehensive solution that addresses both endpoint management and third-party log integration. Specifically, we are seeking a tool and partner capable of:

•Endpoint Management and Incident Response: Leveraging both automated/orchestrated methods and direct interaction to contain and mitigate security incidents. This includes isolating endpoints and user accounts identified as highly likely to be compromised or actively involved in a security event. facilitating process execution chains, registration, registry modifications, and related file activity (write, copy, delete) on the endpoints.

•Third-Party Log Ingestion and Archival: Collecting, storing, and managing all security-relevant logs from third-party systems to ensure optimal visibility into our environment. This capability is critical for effective threat detection, investigation, and compliance with the latest CJIS Security Policy and other regulatory requirements. Currently, CJIS Security Policy requires us to maintain security-relevant logs for one year.

1d.) Do you have an estimated ingest per day and logs per second count? We currently have approximately a daily messages-per-second (MPS) ingest rate of 2500. It is important to note, this is far under what we actually need as we are not able to send our workstation logs to the SIEM. We anticipate an actual MPS of being closer to 4K or 5K.

1e.) Are your hot and cold storage requirements for incidents and or all logs? All security relevant logs so as to meet CJIS Security Policy 1 year retention requirements.

1f.) How do you collect telemetry from your networking devices today? Currently, we have network device logs being sent via syslog to a kiwi server. Firewall logs are sent to Panorama. Network monitoring occurs via Open Manage OpManager. All logs from Panorama and OpManager are being sent to our SIEM and our current MSSP. Logs from the kiwi server are only being sent to our MSSP.

1g.) Do you require cloud detection and response capabilities for AWS? While this was not an original hard requirement, we would prefer solutions that can monitor AWS and other common IAAS providers as we anticipate needing to be able to move into that space in the near future.

1h.) Do you have other technologies/work flows you'd like to automate with SOAR? Our current requirements focus on the core security operations tasks outlined in the RFP. However, we aim to expand the use of SOAR to encompass a broader range of security operations and, where feasible, non-security IT operations. Below is a list of additional potential use cases we are considering for partial or full implementation with SOAR. These include, but are not limited to (note – we list a use case and the current tools we have that we think may be involved in the SOAR solution):

•**Phishing Email Investigation and Response**
(Mimecast Email Security Gateway, Exchange Online, M365 Entra ID, PowerAutomate)
•**Malware Detection and Containment**
(Mimecast Email Security Gateway, Rapid7 InsightVM, MECM/SCCM, InTune)
•**User Account Compromise**
(M365 Entra ID, Active Directory on-prem, Exchange Online, PowerAutomate)
•**Vulnerability Management**
(Rapid7 InsightVM, MECM/SCCM, Patch My PC)
•**Threat Hunting**
(Mimecast Email Security Gateway, Rapid7 InsightVM, Cisco routers and switches, Cisco ISE)
•**Data Exfiltration Detection**
(Cisco routers and switches, Cisco ISE, M365 Purview, Mimecast Email Security Gateway)
•**Ransomware Response**
(Veeam, M365 Entra ID, InTune, MECM/SCCM)
•**Insider Threat Management**
(M365 Entra ID, PowerAutomate, Cisco ISE, Exchange Online)
•**Endpoint Detection and Response**
(Cortex XDR, MECM/SCCM, InTune, Rapid7 InsightVM)
•**Threat Intelligence Automation**
(Mimecast Email Security Gateway, Cortex XDR, Rapid7 InsightVM, Cisco ISE, PowerAutomate)
•**Application Deployment**
(MECM/SCCM, InTune, Patch My PC, PowerAutomate)
•**Patch Management**
(MECM/SCCM, Patch My PC, InTune, Rapid7 InsightVM)
•**System Health Monitoring**
(Open Manage OpManager, VMWare VCenter, Veeam)
•**Access Provisioning**
(M365 Entra ID, Active Directory on-prem, ServiceNow, PowerAutomate)
•**Incident Management**
(ServiceNow, Cisco routers and switches, Cisco ISE)
•**Backup Failure Alerts and Resolution**
(Veeam, Open Manage OpManager)
•**Configuration Compliance**
(Rapid7 InsightVM, Cisco routers and switches, MECM/SCCM)
•**Service Request Fulfillment**
(ServiceNow, PowerAutomate, Exchange Online, SharePoint)
•**Password Reset Automation**
(M365 Entra ID, Active Directory on-prem, PowerAutomate)
•**Asset Inventory Updates**
(ServiceNow, MECM/SCCM, Open Manage OpManager)

2.) Is El Paso County open to keeping pieces of their existing infrastructure such as Log Rhythm or is the county wanting to replace all infrastructure?

2a.) While we are neither against nor in favor of a new LogRhythm/Exabeam solution, we are strongly not in favor of keeping the current platform on-prem in its current state. It is not able to handle the amount of log data and processing load we want to throw at it. Also, we do not want to be in the business of actively managing an on-prem SIEM. We have a smaller staff and need to have those resources focused on using the SIEM rather than

maintaining the SIEM. The current deployment is overly rigid and difficult (and costly) to upscale.

3.) Would an extension to the due date be possible?

3a.) Yes, a one week extension has been granted.

4.) Did the County work with a consultant to create the RFP? If so, who is the consultant?

4a.) We created the RFP and had it reviewed by Information Security and Acquisitions professionals at Gartner to ensure we were aligned with current industry best practices.

5.) Has the County seen any demonstration or done any proof of concepts for security solutions related to this RFP?

5a.) Yes. Over the last year the County has conducted numerous demonstrations with a myriad of different vendors in an effort to understand the current market offerings at a basic level and to help inform ourselves of any capability gaps we have in our current tool set.

6.) We noticed that on page 31, the RFP requires “fully complying” with the requirements listed above, which impacts how we structure your contract, our terms of service, and more. In a perfect world RFP requirements would fit neatly within the specialized scope of a vendor such as Red Canary, but there are conversations and revisions likely required to achieve the results you are looking for. Are you looking for us to begin said legal discussion now to find mutually agreeable language or full compliance with language as required?

6a.) Negotiations of requirements and/or terms and conditions will not occur until an intent to award has been announced after the evaluation period. Submitting vendors will need to include any exceptions to specs, scope, or terms/conditions per the RFP and attached example professional services agreement with their submittal.

7.) In our previous discussion all the initiatives were to be completed by at least 2 vendors. In this response if there are pieces that we can not hit are you open to a multi-source approach. If so, do you have recommended partners we should be working with, should we leave those spots blank or put in who we would recommend to fill those gaps? Do you want us to be working with a Value added reseller to pull in multiple vendors together to fill in all the gaps? If so, do you have a preferred Value added reseller we should work with?

7a.) The County is not award of any previous discussions with any vendor regarding a requirement to involve at least two vendors. A multi-source approach is acceptable under the following conditions:

All sub-contractors must be clearly identified within the proposal.

Each sub-contractor must provide credentials equivalent to those required of the prime contractor as evidence of their ability to successfully execute the scope of work.

Sub-contractors must meet all technical, and security requirements outlined in the RFP.
It is essential that all proposed sub-contractors demonstrate not only their technical capabilities and past performance but also their ability to meet the County’s security standards and compliance expectations. Additionally, because this is a competitive RFP, there is no requirement to engage a particular Value-Added Reseller (VAR). Proposers are encouraged to recommend partners to fill any gaps in their proposal; however, such recommendations must comply with the criteria outlined above.

8.) From the previous question if you do not have a partner or VAR you want us to work with. Are Vendors expected to respond to this RFP, is there an exception that a vendor must meet all listed requirements? For instance if we are able to meet 90% of the requested services, that will disqualify us from selection.

8a.) Vendors are expected to respond to the RFP with their best proposals based on the listed functional requirements. While meeting all of the functional requirements outlined in the RFP is ideal, proposals that do not fully meet 100% of the functional requirements will be reviewed and considered.

In such cases, vendors are encouraged to clearly identify which requirements they can meet and provide justifications or alternative approaches for any unmet requirements. This transparency will help the evaluation committee evaluate the proposal against overall needs and priorities.

Please note that the selection process will consider how well the proposal aligns with the County's critical needs, the vendor's ability to meet the most essential functional requirements, and overall value to the organization.

9.) Are you looking for vendor to fully deliver on Incident Response?

9a.) We are seeking a partner who can assist in executing as many components of the incident response process as possible, while complementing and extending the capabilities of our internal InfoSec team. It is important to clarify that we are not outsourcing our entire information security function. Instead, we aim to establish a collaborative partnership that enhances our capacity to detect and respond effectively to security incidents.

At a minimum, we require a partner with the expertise and capability to rapidly detect, correlate and fully contain security incidents within our enterprise environment, ensuring swift and effective mitigation of potential threats.

To ensure a comprehensive evaluation, we encourage vendors to clearly articulate which components of the incident response process they can support and any areas where they may have limitations. This transparency will help us better understand how your capabilities align with our needs and provide a clearer picture of what a partnership would look like in practice.

10.) Please supply more details regarding the following Playbook scenarios. Step by step playbook tasks would be helpful. a. Ransomware investigation and response b. Phishing investigation and response c. Malware alert investigation and response d. Suspicious authentication attempts (e.g. impossible level, suspicious MFA registration, usual login times)

10a.) We understand the importance of detailed playbooks in incident response and their role in ensuring consistency and efficiency. However, we believe that the formulation of detailed, step-by-step playbooks is best developed in collaboration with the awarded vendor to ensure alignment with both industry best practices and the specific needs of our organization.

At present, we acknowledge that our existing playbooks may be immature or incomplete, and one of our primary objectives in this engagement is to work with a partner who can help us refine and mature these processes. Providing task-by-task playbooks at this stage would not reflect the comprehensive, collaborative approach we are seeking to achieve through this partnership.

We encourage vendors to describe their methodology, tools, and expertise in developing or refining playbooks for scenarios such as ransomware, phishing, malware, and suspicious authentication attempts. Vendors are also welcome to formulate their response based on the technology, vendors, and products disclosed in our RFP to demonstrate how their approach aligns with our current environment.

Should a vendor be selected as our partner, we will provide our existing playbooks and collaborate closely to develop mature, detailed processes tailored to our organization's requirements.

11.) Are you looking for full MDR Services around your current EDR tool?

11a.) Our current preference is to continue using Cortex XDR as our EDR tool. However, we remain open to considering alternative solutions. Vendors proposing a different EDR solution must provide a comprehensive proposal that includes:

•Cost Transparency: All associated costs must be detailed, including professional services for initial deployment, configuration, and ongoing support.
•Justification for Alternative: A clear articulation of why their proposed EDR tool is a superior option compared to Cortex XDR, supported by objective data such as performance metrics, independent evaluations, or case studies.

This approach ensures we can make an informed decision based on both cost-effectiveness and the ability to meet our operational and security requirements.

12.) Is your current EDR tool both MS Defender and Palo Alto XDR? Are you keeping the current vendor or possibly changing?

12a.) We apologize for any confusion. In this context, when referring to Microsoft Defender, we are specifically addressing the Defender capabilities within M365, such as Microsoft Defender for Office 365 and Exchange Online Protection (EOP). For clarity regarding our Endpoint Detection and Response (EDR) solution, please refer to our response to question 11, which outlines our current preference for Cortex XDR and our openness to considering alternative tools under certain conditions.

13.) How does the county feel the current SIEM solution fails to leverage automation and orchestration (LR Smart Response offers some levels of automation and orchestration)? What SOAR capabilities is the county seeking beyond the ones included with their current solution?

13a.) The County recognizes that while LogRhythm's SmartResponse, as currently deployed in our environment, provides basic automation capabilities, it does not fully address our evolving security operational requirements. Modern Security Orchestration, Automation, and Response (SOAR) platforms offer a more comprehensive range of features, broader integrations, and greater operational efficiency than what is achievable with SmartResponse alone.

To maximize the capabilities of our current solution, SmartResponse requires coupling with AIE (Advanced Intelligence Engine) alerts. However, both SmartResponse and AIE have proven to be cumbersome for our analysts and engineers to manage effectively. AIE, in particular, imposes significant resource demands—both in terms of system performance and manpower—which makes the current deployment unsustainable and insufficient to meet the County's needs.

We are open to exploring advancements in LogRhythm/Exabeam's current offerings as their capabilities may have improved since our initial deployment. However, our priority is to adopt a solution that provides robust features, seamless usability, and efficiency enhancements for our security operations team.

14.) Most MDR providers leverage their own Identity Provider to provide secure access to a hosted solution, this allows for them to remain compliant with things like SOC 2 Type 2 and ISO27001 certifications. Would the County be open to allowing the MDR provider to manage their users' access to the hosted tools being provided?

14a.) The County's Identity Provider (IDP) requirement applies specifically to ensuring secure access for our personnel to our instance of the vendor's solution. We understand and accept that back-end administrative access for the vendor's personnel in a cloud-hosted or externally managed environment can and should be handled using the vendor's own IDP to maintain compliance with certifications such as SOC 2 Type 2 and ISO 27001.

We do not intend to require vendors to alter their internal authentication processes. However, the proposed solution must allow the County to securely manage access for our users using our tools and IDP. Proposals should clearly identify where integration with M365 Entra ID is supported for authentication, SSO, MFA, and SCIM provisioning.

If there are areas where integration with M365 Entra ID is not feasible, vendors should clearly outline those limitations and propose alternative methods for the County to securely manage user access. While this single requirement is not intended to unilaterally disqualify any respondent, it will be considered as part of our evaluation. If two offerings are otherwise identical, the solution that more closely aligns with the RFP requirements in this area may receive a higher score from the selection panel.

15.) Are there any additional systems or devices that you expect to add to the scope in the next 6-12 months, or is the current list representative of the full range?

15a.) The current list is representative of the County's primary scope for this RFP. However, there is a possibility that the County may expand monitoring to include cloud infrastructure components, such as AWS and Azure, within the next 6-12 months. This potential expansion is contingent on prioritization and funding approval by senior leadership and is not guaranteed at this time.

Vendors are encouraged to utilize the provided response sheet to outline any optional features or capabilities that support scalability to meet future needs, including cloud infrastructure monitoring. Additionally, vendors should clearly specify any associated costs the County may incur if such optional features are implemented at a later date. This transparency will enable the County to fully evaluate the solution's ability to adapt to changing mission requirements and the evolving threat landscape.

A strong proposal will demonstrate comprehensive coverage of the systems and devices currently defined in the scope. An even stronger proposal will provide clear pathways for scalability and adaptability to address future needs without significant operational disruption.

16.) Can you clarify how your current IT infrastructure is segmented across different environments (e.g., on-premises, cloud, hybrid)?

16a.) The majority of the County's IT infrastructure is hosted on-premises across multiple facilities in El Paso County, Colorado. The County operates two primary data centers in Colorado Springs, which house most of the server infrastructure. These data centers, while geographically dispersed, currently function as a unified active-active distributed environment, operating as a logically single data center.

Many, though not all, County facilities are directly connected via County-owned fiber paths, ensuring high-speed and reliable connectivity. Other facilities utilize Lumen Metro Ethernet (MoE) or site-to-site VPNs to connect to the County's network infrastructure.

In terms of cloud services, the County maintains a hybrid M365 environment, with on-premises domains synchronized to M365. Additionally, the County has an IaaS presence in AWS, supporting specific workloads.

For endpoints, the County operates as a hybrid organization with several thousand laptops deployed across various departments. The distribution of remote versus on-premises work varies significantly by department (e.g., Sheriff's Office vs. IT). Current County policy allows many employees to work remotely two days per week, with three days spent in the office.

17.) Approximately how many users are active in your Active Directory (on-premises), EntraID, and M365 environments?

17a.) The County currently has approximately 5,000 users in both environments.

18.) How many sites/locations are in scope within the El Paso County environment that providers will be monitoring?

18a.) 35.

19.) What SIEM solution is the County currently leveraging? Do you have an average GB/day or EPS (Events Per Second) that you could share?

19a.) The County is currently leveraging LogRhythm SIEM. As noted in the RFP document, our current deployment ingests approximately 2,500 messages per second (MPS). However, this deployment does not capture all desired log sources. We anticipate that the actual MPS, with full log source integration, would be closer to 4,000–5,000 MPS.

We encourage all respondents to propose solutions that either already meet our anticipated demand or can easily scale to accommodate this level of log ingestion to ensure future scalability and operational efficiency.

20.) Can the County team please help define their expectations around “full SOAR capabilities”?

20a.) The County's expectations for "full SOAR capabilities" include a robust platform that enables comprehensive Security Orchestration, Automation, and Response. The following key capabilities define our expectations:

•**Broad Integration Support:** Seamless integration with our existing IT and security stack, including M365 Entra ID, Active Directory, Exchange Online, Mimecast, InTune, MECM/SCCM, ServiceNow, Rapid7 InsightVM, Veeam, Cisco ISE, AWS, VMware vCenter, and other critical infrastructure components.
•**Advanced Automation:** Ability to automate repetitive and time-consuming tasks such as phishing investigations, malware containment, account compromise remediation, and vulnerability prioritization and patching, reducing reliance on manual intervention.
•**Dynamic Playbooks:** Support for flexible, dynamic playbooks that adapt to real-time conditions and can incorporate conditional logic for complex scenarios.
•**Scalability:** The solution must be able to handle current operational requirements, with the ability to scale to meet future needs as threat landscapes evolve or new systems, such as additional cloud workloads, are brought into scope.
•**Intuitive Interface:** A user-friendly interface for security analysts, enabling efficient management of incidents, investigation workflows, and reporting without extensive customization or technical overhead.
•**Threat Intelligence Enrichment:** Real-time integration with threat intelligence feeds and the ability to enrich alerts with actionable context, improving decision-making.
•**Centralized Incident Management:** Unified management of incidents across all log sources with automated escalation, assignment, and resolution tracking to enhance collaboration and accountability.
•**Compliance and Audit Support:** Capabilities to maintain logs, incident histories, and reports aligned with compliance requirements, such as SOC 2 Type 2, CJIS, and HIPAA, with minimal manual effort.
•**User Access Management:** Full integration with M365 Entra ID for authentication, SSO, MFA, and SCIM provisioning, ensuring secure and streamlined user access.
•**Flexibility for Custom Use Cases:** The ability to build custom workflows and integrations to address unique security and operational requirements.

Current Limitations of Our Existing Solution:

The County currently utilizes LogRhythm SmartResponse coupled with their AIE functions, which when combined offer very rudimentary automation capabilities. However, in its current deployment:

•**Integration Gaps:** The platform, as deployed currently, does not support the breadth of integrations expected in a modern SOAR solution.
•**Resource Intensive:** Features such as AIE (Advanced Intelligence Engine) are cumbersome to manage and impose significant resource demands.
•**Limited Scalability:** The current solution does not easily scale to accommodate new log sources or anticipated higher message ingestion rates.
•**Workflow Efficiency:** Analysts find managing SmartResponse and AIE alerts challenging, reducing overall operational efficiency.

The County seeks a modern SOAR platform that addresses these limitations while providing a scalable, efficient, and comprehensive solution to support our security operations today and in the future.

21.) Would a response action to disable a user account leveraging the County’s Identity Provider, EntraID, suffice as a response action for a true positive phishing incident?

21a.) While disabling a user account leveraging the County's Identity Provider, Entra ID, can be a necessary response action in a true positive phishing incident, it is insufficient as a standalone measure. Effective incident response requires a comprehensive approach tailored to the situation, including but not limited to the following actions:

•**Email Analysis:** Examine the malicious email for payloads, links, and other indicators of compromise (IOCs).
•**User Activity Review:** Determine whether the user interacted with the email, such as clicking on links or downloading attachments.
•**Endpoint Investigation:** Check the user's endpoint for EDR alerts, unauthorized changes, or signs of compromise.
•**Web Activity Monitoring:** Review the user's web activity to identify visits to malicious sites linked to the phishing email.
•**Network Traffic Analysis:** Inspect network traffic for indicators such as command-and-control (C2) communication, data exfiltration, lateral propagation, or follow-on attacks.
•**Email System Remediation:** Purge related malicious emails from the system to prevent further compromise.

•**Broader User Checks:** Assess other users who may have received the email to determine if similar actions were taken or if additional accounts are compromised.

•**Administrative Tasks:** Ensure all necessary administrative actions are taken, such as:
•Opening tickets in the County's ServiceNow system to track the incident.
•Sending alerts and updates to relevant stakeholders and technical teams.
•Updating and closing tickets once the incident response actions are completed.

Every phishing incident is unique and should be approached with a combination of these investigative, remedial, and administrative steps to ensure a thorough and effective response. This comprehensive approach not only mitigates the immediate threat but also helps prevent further compromises and strengthens the County's overall security posture.

22.) Typically, Incident Response Retainers are included within in an organization's Cyber Insurance carrier. Does the County currently have this included with their Cyber Insurance today?

22a.) Yes, the County currently has a cyber insurance carrier that includes an Incident Response Retainer. Vendors are reminded that, to be awarded a contract for these services, they must meet all insurance requirements outlined in the Insurance Checklist provided in the RFP.

23.) Questions regarding RFP-25-007 NEXT GENERATION INFORMATION SECURITY OPERATIONS TOOLS AND SERVICES: 1. Can the MDR solution leverage its own tools for EDR/XDR and Vulnerability Management? Instead of Palo Alto Cortex and Rapid7 Insight VM. 2. Under functional requirements the county calls out support for Cisco Firewalls & Palo Alto Firewalls, is the county looking for managed infrastructure services as well? 3. What is the county using today to monitor/log your cloud infrastructure? 4. For the 10TBs of archived data, does that need to be stored for 90 Days for 13 Months? 5. How many enabled Active Directory accounts does the county have?

23a.)

1. Can the MDR solution leverage its own tools for EDR/XDR and Vulnerability Management? Instead of Palo Alto Cortex and Rapid7 Insight VM.

The County is open to MDR solutions that leverage their own tools for EDR/XDR and Vulnerability Management, provided these tools meet or exceed the functional and security requirements outlined in the RFP. Proposals must clearly demonstrate how the proposed tools align with the County's operational needs and security objectives. While the County currently utilizes Palo Alto Cortex and Rapid7 InsightVM, alternative solutions will be considered if they provide equivalent or superior functionality and ease of integration with our existing infrastructure. Any additional costs associated with new EDR/XDR/VM tools must be clearly identified in the RFP response sheet.

2. Under functional requirements the county calls out support for Cisco Firewalls & Palo Alto Firewalls, is the county looking for managed infrastructure services as well?

A point of clarification: while the County has Palo Alto Firewalls and Cisco route, switch, VoIP, ISE, and WiFi – the County does NOT have Cisco Firewalls. The County is not explicitly seeking managed infrastructure services as part of this RFP. However, support for Cisco network devices and Palo Alto firewalls is a functional requirement for monitoring, alerting, and integration with the proposed solution. Vendors may include optional managed infrastructure service offerings in their proposals, but these will not be a primary evaluation criterion.

3. What is the county using today to monitor/log your cloud infrastructure?

The County currently does not have a dedicated tool for monitoring and logging cloud infrastructure. Limited logging and monitoring are performed using native tools provided by AWS and Azure. As stated in the RFP, the County is interested in exploring solutions that can extend monitoring capabilities to include cloud infrastructure, contingent on future prioritization and funding.

4. For the 10TBs of archived data, does that need to be stored for 90 Days for 13 Months?

For the 10TB of archived data, the requirement is to retain data for 90 days of hot storage and 13 months of total storage across warm, cold, and frozen tiers. Proposals should clearly specify how the solution meets these retention and tiering requirements.

5. How many enabled Active Directory accounts does the county have?

5,000

Signature below indicates that applicant has read all the information provided above and agrees to comply in full. This addendum is considered as a section of the Request for Proposal and therefore, this signed document shall become considered and fully submitted with the original package.

PRINT OR TYPE YOUR INFORMATION

Company Name: _____ Fax: _____

Address: _____ City/State/Zip: _____

Contact Person: _____ Title: _____

Email: _____ Phone: _____

Authorized Representative's Signature: _____ Date: _____

Printed Name: _____ Title: _____

Email: _____ Phone: _____