Addendum No. 1 (issued on January 31, 2023) to the

Request for Information Solicitation #2223-23

Answers to Questions received through January 30, 2023

These questions are structured to match the organization of the RFI. Questions from different vendors are commingled here.

Linked questions and answers appear in one box together.

- Answers are written in *italics*.
- When multiple questions receive one answer, the questions are grouped in one box.

Remember that you must submit the Addenda Acknowledgement form with your submission: https://www.urbanaillinois.us/sites/default/files/attachments/Urbana_Illinois-Acknowledgement_of_Addenda_Form.pdf

Terminology Note/Goals for the City of Urbana

Q: "…act automatically on detected threats" – What is the extent of action being requested? (I.e. Stopping a threat automatically, creating a notification to Urbana security staff, etc.) *A: We want the solution to first stop the threat automatically and second to notify Urbana staff after the threat is neutralized. There could be a hierarchy of rules in place that indicate that some threats may only notify Urbana staff, but the primary goal of this solution is "An always-on NDR tool that neutralizes threats…" (Page 1, goal #1).*
Q: 'logging solution' – What is the definition of 'logging solution'? *A: Trying to avoid a circular definition, we consider a logging solution to be software that creates and ingests a history of events (a log) and stores it for future use. Those log entries could original from other locations – like an endpoint. Goal #2 states "…to provide a history of activity in case an event requires research" and question #14 describes using the log "for the forensic analysis of an incident." In questions 12 – 14, we want YOU to tell us what your product does to achieve these goals.*
Q: 'Ongoing penetration testing and vulnerability scanning of unpatched software' – Is this a function required of the 'NDR' solution? *A: It is not required. We have been told that some NDR solutions probe vulnerabilities in various ways. If the solution provides those features, it is a benefit – but please note that this was goal #5 and the goals were listed "… in order of importance" on page 1.*

Project Budget

Q: I noticed the budget is for fiscal year ending June 2023. Is the stated budget an expected yearly budget? Implementation would certainly be a portion of that up front, but curious what the monthly/yearly budget constraints might be.

A: The $55,000 budget includes the implementation and first year's license cost. In future years, we expect to only pay for renewals. We will set those budgets appropriately, based on the solution pricing.

Q: Is there any wiggle room on the budget or is a firm $55,000?

A: The IT Division has discretion to move money between contractual and supply budget lines. However, we do not have the authority to create budget authority where it did not exist already. So a higher-priced solution would need to justify the additional cost, because it will be pulling budget away from other IT initiatives.

City IT Background

Q: I noticed 2 domains were mentioned - the City and the Park District. We can monitor both, however the data for the 2 locations would be intermingled. Do you have any compliance/business requirements that would require these to be separate?

A: The City's network includes the Police Department, so it is subject to Criminal Justice Information Systems (CJIS) compliance. This does not require that the monitoring of the two domains needs to be separate, but it does mean that all intermingled data needs to be managed to CJIS standards.

Q: Do all network domains have the same ingress/egress points for internet connectivity?

A: Yes.

Q: From reading the RFI, I am assuming that you have 2 physical networks. Is that correct?

A: The City has one network with multiple off-site subnets.

Q: What is meant by 'integrate with Crowdstrike Falcon'? Does this mean not conflict with Crowdstrike Falcon?

A: Not conflicting with Crowdstrike Falcon would be the <u>minimum</u> expectation. We would like a solution that ingested the output from Crowdstrike Falcon to be aware of an incident that (for example) impacted multiple endpoints with the same event. The individual installs of Crowdstrike Falcon wouldn't be aware of each other, but we would hope that the NDR would "see" the relationship between multiple endpoints.

Q: Are you willing to fill out an online scoping document that provides details [on] your environment? This document will allow us to understand the amount of online storage needed and thus allow us to properly price the solution?

Q: Can you share how many servers you have (physical and virtual) for both the City and the Park District? For virtualized environment, do you use Hyper-V or VMWare?

Q: How many total locations are there between the City and the Park District?

- Do each of these locations have internet egress or do any backhaul through a main location?
- Is there a firewall at each of these locations?
    a. Any high availability pairs?
    b. What is the vendor(s)?
    c. What is the physical handoff between the firewall and core switch at each location (i.e., 1G Copper, fiber, etc.)?
- What is the internet bandwidth at each of these locations?

Q: Can you please provide me with (the total number of devices) so that we can price the (proposed solution) accurately?

A: We will not be disclosing details about our environment in a publicly available document. For those solutions that submit a response and are selected for the next phase, we will provide more details. (See the RFI, page 2, step 3b.) ***Responses to this RFI are not expected to provide exact pricing for the City. Instead, we want to know the components of your pricing. For example, if you price by endpoint then tell us the price per endpoint.***

Submittal Instructions / Terms and Conditions

Q: Did you have a Q&A window for us to ask questions about the RFI should we need clarification?

A: Our standard is to answer all questions received more than 5 working days before the end date. ***So we will answer all questions received before 5 PM on Tuesday February 7.*** *Thank you for helping us clarify this.*

Logging

Q: Is direct access to the data logged required?

*A: Direct access is not needed as long as we **can** access the logged data when necessary. The answer to question #14 should describe how we would access and extract the logs, for example to share with an auditor, our insurance company, a state or federal agency working with us, etc.*

Q: Do you have any requests for how long logged data needs to be accessible? 30, 60, 90 day logs, or longer?

A: The FBI's Criminal Justice Information Services (CJIS) Security Policy says that "The agency shall retain audit records for at least one (1) year." (see section 5.4.6 here: https://le.fbi.gov/cjis-division-resources/cjis-security-policy-resource-center) So, the answer is "at least one (1) year".

Pricing

Q: Under Pricing, item 29, is the City of Urbana requiring the purchase go thru one of the listed Procurement Cooperatives? Or is the city indicating that using Purchasing Cooperative is a way to avoid RFP, but if there is no Purchasing Cooperative agreement in place an RFP will be posted?

A: Our process is described on page 2 – in particular see steps 4 and 5. We do not require that the purchase go through a Procurement Cooperative.

Q: Can you please recommend any resellers that we can reach out to who are part of one of the cooperatives? We would be willing to submit a proposal through a qualified reseller.

A: The links that follow take you to a list of contract-holders. Not all of these might be appropriate as re-sellers, but some are:

- *Sourcewell: https://www.sourcewell-mn.gov/contract-search?category=10766&keyword=*
- *TIPS-USA: https://www.tips-usa.com/vlist.cfm*
- *Omnia: https://www.omniapartners.com/publicsector/suppliers/odpbusiness/contract-documentation#c45661*
- *HGACBuy: https://hgacbuy.org/contracts*

Q: Are you willing to accept an optional services section on the bid? As we read through the RFP some of the questions lead towards solution outside of a standard NDR.

A: Yes, but as requested in Question #28: "If modules can be implemented separately, price each and identify which are required and which are optional."