Cybersecurity Request for Proposals

Pre-Bid Conference Held June 16, 2023

Questions and Responses

The New York State Unified Court System (UCS) thanks the vendors that submitted the questions below concerning the Cybersecurity Request for Proposal (RFP) during the pre-bid conference held on June 16, 2023. The questions and responses were transcribed from the audio recording of the pre-bid conference. They have been reproduced here and edited for brevity, clarity, and responsiveness. Any clarifications or additions to answers provided during the pre-bid conference have been noted in the response.

Below are the questions UCS received during the pre-bid conference and the responses thereto.

1. What is the new due date for proposals?

   ***UCS Response*: July 11 at 3:00 PM Eastern.**

2. The RFP mentions the Splunk SOAR component. Is it critical for the response to this RFP?

   ***UCS Response*: Yes.**

3. Our SOC uses a different sort of technology, meaning we would fetch alerts out of your Splunk instance for our alerting and response. Can we use both?

   ***UCS Response*: No, you are not allowed to take that data to your SOAR You would be specifically working in [UCS's] Splunk environment using Splunk SOAR and creating the alerts within [UCS's] environment with [UCS's] Splunk SOAR.**

4. Regarding the price form, can you define your expectation for the one-time onboarding, meaning the number of months and how does that impact the way we price the first full year?

   ***UCS Response*: UCS expects onboarding activities to take up to three (3) months from the creation of the awarded contractor's Splunk account. It is up to the bidder to determine how such activities impact pricing for the first full year.**

5. How does that (referring to the previous question) impact the way we price the first full year?

   ***UCS Response*: To the extent there are costs pertaining solely to onboarding activities during the first year of the contract resulting from**

this RFP, those costs should be specified in the Pricing Sheet's row for "One-time onboarding costs" and they should <u>not</u> be included in the row for "Security operations center (SOC) services."

6. Is managing 2,500 firewall intrusion detection systems across the bidder's aggregate customer base a hard requirement?

   <u>UCS Response</u>: Yes. As set forth on page 4 of the RFP, Minimum Qualification # 2 is: "The bidder currently monitors a minimum of 2500 firewall/intrusion detection systems (IDS)/intrusion prevention systems (IPS) devices across its aggregate customer base."

7. How does Section 4.2 price adjustment factor into how we show our price?

   <u>UCS Response</u>: Section 4.2 price adjustment refers to the awarded contract pricing in the optional renewal terms and not to bid response pricing.

8. The mandatory requirement lists the Fed ramp solution. How is this relevant to the UCS on premises solution? Or is the intent to propose a solution that may go to the cloud?

   <u>UCS Response</u>: UCS is requiring FedRAMP compliance to ensure, among other things, that data remains in the United States and that metadata taken from UCS ticketing systems will have appropriate safeguards. UCS deems all data stored on systems not on UCS premises to be cloud-based, and UCS therefore requires the awarded contractor to comply with FedRAMP protocols.

   Note: Formal FedRamp certification is not required but formal SOC2 certification is. If a formal FedRamp certification is not available, the vendor must be able to demonstrate compliance through provision of a third-party (e.g., Qualys, Tenable, etc.) scan report acceptable to UCS accompanied by a self-attestation of compliance. The report must be provided within 30 days of bid opening and any Awarded Contractor must demonstrate continued compliance throughout the term of the resulting contract. As indicated in Article II of the RFP, "The proposed solution must comply with Systems and Organization Controls 2 (SOC 2®) requirements" and "The proposed solution must comply with Federal Risk and Authorization Management Program (FedRAMP®) Moderate or High Impact Level Security Controls Baseline." See Mandatory Requirements # 1 and # 3, respectively.

9. The SOC2 and FedRAMP requirements seem like those would be requirements for the vendor's infrastructure; however, it sounds like with this contract, which seems to be staff supplemental, we're not quite sure how our internal infrastructure for other customers is relevant if you're just looking for us to provide analysts.

***UCS Response*: UCS is requiring SOC2 and FedRAMP compliance to ensure, among other things, that data remains in the United States and that metadata taken from UCS ticketing systems will have appropriate safeguards. UCS deems all data stored on systems not on UCS premises to be cloud-based, and UCS therefore requires the awarded contractor to comply with FedRAMP and SOC2 protocols.**

10. How many Splunk licenses are available for the vendor? Are you expecting the vendor to provide SOAR licenses for their resources to access the UCS environment?

    ***UCS Response*: During the pre-bid conference, UCS responded that it intends to supply one license for the awarded contractor. UCS has not yet determined whether each of the awarded contractor's analysts and engineers needs an individual license or whether one license for all of the awarded contractor's staff is sufficient.**

    Upon further review, UCS will create enough accounts in the Splunk ES SIEM for the awarded contractor's analysts, and UCS will designate a sufficient quantity of SOAR licenses as determined by UCS in its sole discretion for awarded contractor's use during the term of the contract resulting from this RFP.

11. Do vendors have to be local in New York can they be remote in the continental United States?

    ***UCS Response*: The awarded contractor and its employees and/or subcontractors must be in the continental United States. See Section 5.3 of the RFP on pages 11-13. The awarded contractor does not need to be located in New York State.**

12. Does UCS expect the contractor to perform all back end engineering of Splunk Enterprise, including components that address requirements such as Splunk architecting and/or Splunk administration, such as patching and updating?

    ***UCS Response*: The awarded contractor will have to patch the Splunk environment as well as update to the latest version of Splunk. The awarded contractor will be responsible for monitoring the health of its Splunk platform to make sure the alerting capabilities don't go down.**

13. Does the patching requirement referenced in the previous question apply solely to Splunk or to the awarded contractor's operating system as well?

    ***UCS Response*: The patching requirement applies only to Splunk.**

14. If the awarded contractor has to patch and administer the back end, then are there specific qualifications around Splunk architecture, or can the contractor change that architecture? If UCS is requiring the contractor to provide

performance, then would the awarded contractor also be able to determine, for example, cluster sizes? How would that work?

<u>UCS Response</u>: UCS would have to make changes to architecture. UCS would have to upgrade the cluster. Since UCS has robust servers and the awarded contractor had recommendations that UCS needed to implement, UCS would work with the awarded contractor to implement those recommendations.

15. Following up on the previous question, does the awarded contractor need to staff anybody accordingly in order to address that part of the collaboration?

<u>UCS Response</u>: During the pre-bid conference, UCS responded, "No."

However, upon further consideration, UCS has determined that the awarded contractor's Splunk engineer may recommend changes to UCS, but there is no expectation that the awarded contractor will be rearchitecting the UCS environment.

16. Is UCS's Splunk license adequate for future anticipated volume?

<u>UCS Response</u>: The UCS Splunk license is adequate for existing needs. If UCS needs to purchase additional licenses, it will do so.

17. Section 4.14 of Exhibit H (NYS Office of Information Technology Services Security Policy No. NYS-P03-002) states all systems must be scanned for vulnerabilities before being installed and production and periodically thereafter. Section 1.1 of the Overview, which is on Page 3, says vendors must include vulnerability management. Please clarify.

<u>UCS Response</u>: UCS will not install on its systems any new software or hardware at the recommendation of the awarded contractor. The awarded contractor will perform vulnerability scans using UCS software.

18. Regarding the estimated 200 instances per week listed in the RFP, it is possible to get a breakdown of the severity of those incidents and the current time to remediate?

<u>UCS Response</u>: It is not feasible for UCS to supply a breakdown of those incidents at this time. Consistent with Component M3 as set forth on page 37 of the RFP, UCS encourages bidders to propose a categorization scheme for incidents as well as to propose reporting on such categorization in the bidder's executive-level reports.

19. How big is the UCS contracting team?

<u>UCS Response</u>: The number of employees working in the UCS Contracts and Procurements Unit is not relevant to this RFP. To the extent the

question asks about staffing level requirements from the awarded contractor, please see Section 5.3 of the RFP on pages 11-13.

20. Does the requirement that the bidder supply at least fifteen (15) employees to the UCS SOC apply only when there is a surge (that is, when there is an actual, critical incident)? In other words, is UCS expecting to have 15 persons actually named for incident response capability or is UCS asking for the availability of 15 people during an incident?

    <u>UCS Response</u>: Staffing levels appear primarily in two sections of the RFP. First, in Section 5.3 (Required Staffing), the selected bidder must provide a contract manager, a service manager, a full-time Splunk engineer, and at least eight (8) qualified security analysts, with at least three of those analysts assigned during the daytime shift, at least three analysts assigned during the evening shift, and at least two analysts assigned during the overnight shift. The RFP states that the responsibilities of the contract manager and service manager may be fulfilled by the same individual. Second, as set forth in Section 5.4 of the RFP (Preferred Components of Bidder's Proposal), the preferred bidder will supply at least fifteen (15) employees to the UCS security operations center; this staffing level reflects UCS's preference and is not a requirement. Accordingly, UCS does not expect the awarded contractor to supply fifteen (15) employees to respond to a surge unless such a response is necessary given the unique circumstances of the incident.

21. How large is the UCS staff for Splunk and the security team in general?

    <u>UCS Response</u>: UCS declines to disclose this information in a public-facing document for security reasons. The awarded contractor will be working with a dedicated UCS team on the implementation of these services.

22. Can we submit a WBS (work breakdown structure) MS (Microsoft) Project file outside of the page count?

    <u>UCS Response</u>: No. The only document expressly excluded from the page limit is the compilation of the bidder's references. See Section 6.2.2. on page 17 of the RFP.

23. Regarding vulnerability scanning, does UCS use Qualys or Tenable? Given that Qualys can automate patching and remediation, would that be available to help the selected bidder or is supplying that capability something bidders should incorporate in their proposals?

    <u>UCS Response</u>: UCS does not have Qualys patching. The awarded contractor will not be patching the UCS environment with Qualys; however, the awarded contractor will patch the Splunk instance UCS provides. UCS only has Qualys, Tenable, and some other tools for vulnerability scanning.

24. Questions regarding the Splunk setup. Are there any visibility requirements around that for the CSO regarding how information should be broken down or where UCS is looking for information for a specific particular district or anything along those lines?

    ***UCS Response*: After execution of the contract resulting from this RFP, UCS and the awarded contractor will discuss playbooks and runbooks as well as what information UCS wants to see in dashboards.**

25. Will UCS share the recording of the pre-bid conference today?

    ***UCS Response*: No. UCS will share the questions and answers from the pre-bid conference during the week of June 19.**

26. It appears that in the initial Q&A, UCS indicated that VMWare is not included in the technology stack; however, it's listed in the current environment in Section 5.1. Please clarify. Is Crowdstrike able to monitor that virtual environment or any potential containers?

    ***UCS Response*: UCS mentioned VMWare in the RFP because UCS has the software for VMWare. Crowdstrike monitors everything on which UCS has endpoints. The awarded contractor is not expected to install VMWare**

27. Follow up to Question # 26: The bidder wants to ensure it provides staff with the skill sets needed for the UCS environment, as well as to ensure that there is no additional scope creep outside of Splunk. Are there other skills sets beyond a Splunk architect, Splunk SOAR developer, and vulnerability management that UCS is expecting?

    ***UCS Response*: The awarded contractor needs to have knowledge of EDR (endpoint detection and response) as well as the skillset applicable for SOC as a service.**

28. Crowdstrike has workflows. Does UCS expect the selected vendor to work inside the workflows?

    ***UCS Response*: Yes.**

29. Follow up to Question # 28: So, will the awarded contractor have access not only to the SIEM (security information and event management) but also to the workflows in the configurations in Crowdstrike?

    ***UCS Response*: UCS will negotiate with the awarded contractor whether to provide access in Crowdstrike. Proposals should explain why the bidder believes such access is necessary and/or beneficial.**

30. Does UCS normally define use cases, then knowledge articles, and then actually push that into UCS's correlation searches? And how does that workflow look in regards to the general methodology?

    <u>UCS Response</u>: UCS creates use cases that UCS implements, but the third-party SOC will have to create their own use cases for their own Splunk instance and then work with UCS to get alerting working correctly.

31. Follow up to Question # 30: And then does UCS utilize the ITSM (IT service management) for those knowledge articles?

    <u>UCS Response</u>: During the term of the contract resulting from this RFP, UCS will utilize its ITSM for those knowledge articles. UCS expects the awarded contractor to provide use cases, playbooks, runbooks for any alert created.

32. Regarding MITRE: has UCS already done a MITRE assessment to identify any gaps that UCS will need to release to the vendor at the time of award?

    <u>UCS Response</u>: UCS will discuss any such assessment with the awarded contractor.

33. Regarding the requirement that the selected vendor supply 15 employees: do those employees have to be on 24 × 7, and how does that relate to the staffing requirement for three employees during certain hours?

    <u>UCS Response</u>: See response to Question # 20.