Cybersecurity Request for Information

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) issued on May 26, 2023.

Below are responses to the questions UCS received in connection with this RFP.

Vendor # 1

Question:

I have looked on the http://www.nycourts.gov/admin/bids website as advised in the announcement for this RFP, but currently, it does not show. If you could forward me the RFP, it would be greatly appreciated.

***UCS Response*: Thank you for your interest. Per your request, please see attached RFP specifications, including Attachment I, Attachment III, and Attachment IV.**

Note - The RFP was posted on the UCS website on the issue date, 05/26/2023. You may have to clear your browser history prior to viewing the "Current Solicitations" on the UCS public website to view it: *http://www.nycourts.gov/admin/bids* . As a reminder, pursuant to the RFP, even though the bid documents has been provided to you upon request via attachment to this email, bidders are solely and wholly responsible for reviewing the respective solicitation and bid documents on the UCS website *http://www.nycourts.gov/admin/bids* regularly, up to the scheduled date and time of the bid/proposal due date, to ensure their knowledge of any amendments, addenda, modifications or other information affecting the solicitation or bid documents in question. UCS reserves the right, prior to bid opening, to amend the RFP specifications to correct errors or oversights or to supply additional information as it becomes available.

Vendor # 2

Question:

I know questions are due on June 9th and we/[Vendor] plan on submitting a few other questions, but we wanted to get one question to you sooner than the others and get UCS' input on it. Perhaps we could get an earlier response to this if possible as we view it as a foundational given our vast experience in delivering these types of services (we did respond to the RFI). The question is: Given that industry standard contracts for SOCs would contain reasonable limitations on damages and limit broad indemnities, is UCS willing to consider mutually agreeable language in Exhibit E sections titled “Indemnity” and “Warranties and Guarantees,” intended to clarify the scope of the indemnities as well as add a limitation of damages?

<u>UCS Response</u>*: Yes, UCS will entertain contract language that clarifies the indemnity and warranty language in Exhibit E to reasonably allocate risk among the parties. Please note that any such language must adhere to the general indemnity/warranty provisions in the RFP and be approved by NYS Office of Attorney General and OSC.

Vendor # 3

<u>Question:</u>

Do the FedRamp and SOC2 compliance requirements require formal certification or self-attestation that we comply with the security controls?

<u>UCS Response</u>*: 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.

Vendor # 4

<u>Question:</u>

Does the solution we provide truly require “us” to manage Splunk? Our solution would allow us to pull your Splunk into our platform, but in the end, it would still be our 24/7/365 Adlumin Managed Services (SIEM, SOC MDR, UNLIMITED LOG INGESTION/RETENTION).

<u>UCS Response</u>*: The Awarded Contractor must manage the Splunk instance that UCS will provide to the Awarded Contractor.

Vendor # 5

Questions:

1. I am inquiring about getting an extension granted for our response to the RFP. We are looking for a one-week extension if possible. Will State of New York Judiciary extend the due date to July 27, 2023?

   ***UCS Response*: After internal review, UCS has extended the bid due date for all bidders to Tuesday, July 11, 2023 at 3:00 PM.**

2. What are the log retention requirements from the SIEM?

   ***UCS Response*: Given the structure of the intended solution, vendor's log retention requirements are not relevant to this procurement. Please note that Awarded Contractor may be subject to other retention timelines and requirements that apply to NYS vendors.**

3. Does the State have Engineering staff to meet their storage requirements?

   ***UCS Response*: UCS engineering staffing levels are not relevant to this procurement.**

4. Does the State have SSL decryption in place?
   a. If yes, is there an IDS monitoring the traffic.

   ***UCS Response to 4 and 4a*: SSL decryption is not relevant to this procurement.**

   b. Are the alerts from IDS fed into Splunk SIEM?

   ***UCS Response*: Yes.**

   c. Are there any threat intelligence feeds into the Splunk SIEM?

   ***UCS Response*: Yes.**

5. How is the State currently receiving Active Directory alerts and logs in to Splunk?

   ***UCS Response*: All logs are ingested into the UCS Splunk environment.**

   a. Is this adequate to meet State's FedRAMP requirements?

   ***UCS Response*: This question is not relevant to this procurement.**

6. Does the State currently collect logs from all assets being monitored?

   ***UCS Response*: Yes.**

7. Is the State currently collecting logs from all of the assets identified in Section V – Scope of Work subsection 5.1 - Current State on page 8 and page 9?

    a. If not, what is the timeline to build out the collection of the logs from all of the sources identified on page 8 and page 9?

***UCS Response to 7. and 7a.**: The UCS currently collects logs from every device.*

8. Will the State share a topology of their environment?

***UCS Response**: For security purposes, UCS will not furnish this information in a public-facing document.*

9. Does the State expect the bidder to provide on-site support?

***UCS Response**: No onsite work is anticipated.*

10. Is the bidder expected to maintain and manage all tools listed in the RPF or just the Splunk SIEM & SOAR platforms?

***UCS Response**: The awarded contractor only has to maintain Splunk SIEM and Splunk SOAR.*

11. There is a contradiction between D5 and the rest of the RFP where it allows bidder to have the Splunk SIEM platform outside of the State's environment.

***UCS Response**: To clarify, the Splunk SIEM platform will not be allowed outside the UCS environment. D5 asks the bidders to describe their organizational capability and not necessarily the bidders' proposed solutions.*

12. Regarding the SLA table, how does the State like to be notified?

***UCS Response**: As indicated on page 51 of the RFP, "Notification methods are based on approved escalation procedures as documented in the SOC/ UCS runbook."*

13. Please provide the number of tickets generated per day?

***UCS Response**: UCS routinely receives over 200 incidents weekly.*

14. What is the current budget for RFP# OCA/DOTCR-131?

***UCS Response**: The UCS does not provide internal budgetary information.*

15. Please provide the number of Severity 1 and 2 (Emergency & Critical) events received per week or month?

    ***UCS Response*: UCS routinely receives over 200 incidents weekly.**

16. Is it the expectation of the vendor to log onto UCS' Splunk environment to deliver its service?

    ***UCS Response*: Yes.**

17. Is the vendor allowed to install equipment it needs to deliver its service on premise in a dmz from UCS?

    a. If so, will the State provide lockable cabinets, etc. or will the vendor need to provide?

    b. How much room will the State provide to the vendor, i.e. 1 cabinet, 2 cabinets, etc.?

    ***UCS Response to 17, 17.a, and 17.b*: Installation of a vendor's equipment is not allowed. Please refer to Mandatory Requirement # 5 on page 4 of the RFP, which states "The proposed solution must integrate with the existing UCS Splunk Security Information and Event Management (SIEM) system (600 GB/day license) and scale up without installation of proprietary vendor hardware" (emphasis added).**

18. Does the State require the vendor use private connectivity (MPLS or Private Line) or public connectivity (IPSec) as the interconnection between the vendor and the State?

    a. If public connectivity, is the vendor able to terminate the tunnel on the State's equipment or must the vendor provide its own equipment?

    ***UCS Response to 18. and 18.a*: UCS will provide the AC with VPN or SSLVPN access to the AC's Splunk instance, which might take several days to configure.**

19. The State asks for the vendor to describe its capabilities to monitor a variety of data sources. Does the State require the vendor to monitor the data sources beyond the ability of the data source to send log data?

    ***UCS Response*: Yes. The Awarded Contractor will monitor all data within the UCS environment as well as relevant external data from other sources, such as the dark web which may provide threat intelligence to the UCS environment.**

20. If the vendor feels there are additional services or recommendations that would benefit the State, can the vendor provide descriptions of those services or recommendations in an Appendix?

***UCS Response*: No. The UCS is only soliciting those services specified in the RFP. Bidders should refrain from proposing optional services.**

21. Can the State provide examples of functions or tasks that would be expected of the vendor?

    ***UCS Response*: The vendor will be performing all SOC duties. For a description of the scope of work see Section 5.2 on pages 9-11 of the RFP.**

22. Is the vendor required to use the State's vulnerability management solution or provide their own?

    a. If the vendor is to provide their own, will the State remove the conflict with Mandatory Requirement #9?

    ***UCS Response to 22 & 22a*: The Awarded Contractor must use the UCS vulnerability management solution.**

23. What is the average annual spend for the State's current Security Operations Center services?

    ***UCS Response*: UCS's current vendor is compensated $187,020 quarterly for an annual contract.**

24. Under Security Services Management, is the vendor expected to implement patches to the UCS' Splunk and data sources?

    ***UCS Response*: The Awarded Contractor will implement patches to the UCS Splunk environment only.**

Vendor # 6

Questions:

1. If it can be proven that a dedicated Splunk Engineer is not required for our service to be effective, is it still considered mandatory?

   ***UCS Response*: A Splunk engineer is mandatory.**

2. Will the Jira system for ticketing allow for API access for ticket automation?

   ***UCS Response*: Yes, Jira has access via API to the UCS Splunk environment.**

Vendor # 7

Questions:

1. Assuming that CJIS environments will be severely restricted in terms of access. What are the limitations inbound or outbound to that environment?

***UCS Response*: No ports will be opened. The selected vendor's Splunk engineer will configure the UCS Splunk environment to the UCS Jira ticketing system to alert the UCS security operations center (SOC). The selected vendor's Tier 1, Tier 2, or Tier 3 analyst will work the alerts and automate in the UCS environment. As stated on page 9 of the RFP, "Data, including event logs and network flow data, remains on UCS premises and does not leave the UCS environment; however, metadata regarding security alerts may be entered into the selected contractor's ticketing system." No data will leave the UCS environment.**

2. Can we open ports to pull or push information from those environments?

   ***UCS Response*: No ports will be opened.**

3. Who are the other providers/partners that we will need to collaborate with for infrastructure and application ownership (e.g. network, provisioning infrastructure, access/onboarding/offboarding, etc.)?

   ***UCS Response*: UCS will give the selected vendor access to the UCS Splunk environment. UCS will create the accounts.**

4. Are there shared state service entities that we will need to interact with?

   ***UCS Response*: No.**

5. Can you list the access requests, background checks, and compliance training that will need to be completed by our team?

   ***UCS Response*: UCS will provide the selected vendor with VPN or SSLVPN access to the vendor's Splunk instance, which might take several days to configure.**

   For information about background check requirements, please consult page 40 of the RFP. Costs for conducting background checks are the responsibility of the selected vendor.

   Regarding training, please see page 13 of the RFP, which states, "The preferred proposal will also include a comprehensive description of how bidder provides initial and ongoing training to bidder's security-monitoring staff; proposals indicating that security-monitoring staff must complete initial training covering security and phishing—and that such training is supplied at least once every six months—will be preferred to proposals with a narrower scope of training or with a less frequent schedule of ongoing training. The preferred bidder will also explain how it maintains required knowledge and skills among its staff, with preference given to bidders that pay for staff training and/or third-party certifications." UCS will evaluate the comprehensiveness of bidders' training programs. See Component # B9 on page 34 of the RFP.

6. Of the data sources listed, is there a known % of each type need to be onboarded into Splunk or should these types of requests be considered ad hoc?

   ***UCS Response*: UCS has terabytes of data daily. For security purposes, UCS will not furnish the requested breakdown in a public-facing document; however, this information will be furnished to the selected vendor upon request and, if required prior to contract execution, completion of a non-disclosure agreement acceptable to UCS in its sole discretion.**

7. How many security incidents do you receive per day (including false positives, benign, suspicious, or malign events). This represents the total number of security related events from all targeted sources (e.g. EDR, Firewall, Network traffic, etc.)?

   ***UCS Response*: UCS routinely receives over 200 incidents weekly.**

8. Have you had a breach of more than 500 records over the past year?

   ***UCS Response*: No.**

9. Past 5 years?

   ***UCS Response*: No.**

10. What are the critical security vendor solutions/appliances that you currently rely upon (e.g., Firewall, VPN, Cloud Security, Email Security, EDR, Vulnerability, Pen Testing, Patch management, WAF. AV, etc.)?

    ***UCS Response*: The selected vendor will work in the UCS Splunk instance creating alerts and notifying the UCS SOC of incidents and working with Splunk SOAR to automate some activities. All UCS devices log to Splunk, and all alerting and reporting of incidents will come from Splunk.**

11. What is your ITSM solution for ticketing and case management (e.g. JIRA, Service Now, etc.)?

    ***UCS Response*: UCS uses Jira and Splunk, and the selected vendor will create automation within the UCS system.**

12. What is your approved instant messaging platform?

    ***UCS Response*: UCS uses Jira and Splunk, and the selected vendor will create automation within the UCS system.**

13. What, if any, is your current SIEM solution?

    ***UCS Response*: UCS uses Jira and Splunk, and the selected vendor will create automation within the UCS system.**

14. Do you have a current SOAR environment?

***UCS Response**: Yes. UCS uses Splunk SOAR.*

15. Do you currently have a DRA plan that allows for enterprise-wide, heterogeneous backup and automated recovery to the point of infection in the case of a ransomware attack?

***UCS Response**: Yes.*

16. What commercial threat list providers do you rely upon currently or are you targeting for this implementation?

***UCS Response**: UCS requires the selected vendor to incorporate alerts from the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Federal Bureau of Investigation, among other sources.*

17. Are any of them providing comprehensive reputation scoring?

***UCS Response**: Yes.*

18. Will you leverage SSO/SAML Integration that is already in place or will it require additional configuration?

***UCS Response**: UCS uses single sign-on (SSO), and it is already in place.*

19. Do you have a current Incident Response Plan (IRP) to address the Incident Response Process as it relates to the system(s)/Application in the cloud environment?

***UCS Response**: UCS has a plan for incident response. The selected vendor should have an incident response plan relating to systems/applications in the cloud environment. Please note that, per page 12 of the RFP, "The scope of work for this RFP excludes onsite incident response (IR) services. UCS currently maintains a relationship with an identified vendor for onsite IR services. The successful [security operation center provider] will, however, need to cooperate with the existing onsite IR services vendor as needed."*

20. Will we be providing managed services to maintain or host your Splunk environment?

***UCS Response**: The selected vendor will maintain and upgrade alerts on the UCS Splunk environment.*

21. Do we need to contribute to or maintain documentation on your WIKI or in the context of an SSP/POAM?

***UCS Response*: Yes.**

22. Do you have automated patching, configuration management, and/or software distribution solutions in place?

    ***UCS Response*: Yes.**

23. Please list the CIDR ranges for any domains you have registered for your organization.

    ***UCS Response*: For security purposes, UCS will not furnish the requested information in a public-facing document; however, this information will be furnished to the selected vendor upon request and, if required prior to contract execution, completion of a non-disclosure agreement acceptable to UCS in its sole discretion.**

24. What are the required processes and methods of remote access to systems to be utilized and/or managed in the NYS Courts environment?

    ***UCS Response*: With few exceptions, UCS does not permit routine remote access and does not allow UCS staff to work from home.**

Vendor # 8

Questions:

1. Section 5.1 - ‘Current State’ includes a list of technologies. What modules were included in the CrowdStrike procurement such as Overwatch, Identity Threat Protection, Falcon Forensics, Essential Support, Firewall Management, Falcon Discover, Falcon Insight, Cloud Workload Protection, Falcon Prevent and/or additional modules not listed herein?

   ***UCS Response*: UCS has all of the specified modules. All logs go to Splunk. The selected vendor will create alerts from the UCS Splunk.**

2. Section 5.1 - ‘Current State’ includes a list of technologies but does not list Enterprise Security. Has UCS procured Splunk Enterprise Security (SIEM requiring separate licensing) to leverage the development of correlation searches and notables?

   ***UCS Response*: UCS has Splunk Enterprise Security (Splunk ES) and Splunk Security Orchestration, Automation, and Response (Splunk SOAR). The vendor will create alerts and automation using the UCS system.**

3. Does UCS currently own the Splunk environment and is it maintained within the VMWare or Azure environment?

   <u>UCS Response</u>: UCS has an on-premises Splunk environment. UCS does not a have a VMWare environment. UCS has multiple dedicated servers for Splunk.

4. Exhibit F - Exhibit F Security Operations Center Terms and Conditions requires “maintaining the mirrored Splunk environment.” What does UCS define as “mirrored” from a licensing, technology stack, and location requirement perspective?

   <u>UCS Response</u>: UCS will furnish the selected vendor with an instance of the UCS Splunk environment on premises that is exactly like the UCS environment. As stated on page 9 of the RFP, “Data, including event logs and network flow data, remains on UCS premises and does not leave the UCS environment; however, metadata regarding security alerts may be entered into the selected contractor’s ticketing system.”

5. What is the uptime of the current UCS Splunk environment and can details be provided on current performance metrics to determine if additional configuration and/or architecture may be required?

   <u>UCS Response</u>: UCS’s Splunk current uptime is 99%. No new architecture is required. As stated on page 10 of the RFP, “UCS will not install any additional software on its systems as part of the SOC solution. All UCS data must remain in systems physically located in the contiguous United States. All work logs will stay on UCS premises.”

6. Section 5.2 of the RFP outlines the ‘Statement of Work’ for the SOC solution and list various data sources. Are the integrations between the sources and the SIEM already established/configured or do additional sources need to be configured?

   <u>UCS Response</u>: The selected vendor will create the automated alerts on incidents that occur. The Splunk instance UCS provides will not be configured by UCS. The vendor needs to configure that instance. All the data sources are in the vendor’s Splunk instance.

7. Section 5.2 of the RFP ‘Statement of Work’ indicates “must create electronic alerts based on defined priority criteria after validation and triage by an SOC analyst.” Does UCS already have defined criteria and/or playbooks the SOC solution must adhere to currently or include in operational procedures?

   <u>UCS Response</u>: UCS and the selected will collaborate on customized playbooks and runbooks based on the best standards in the industry for alerting. Vendors are strongly encouraged to provide these documents with their response as outlined on page 14 in the RFP.

8. In Mandatory Requirements, the “proposed solution must comply with […] FedRAMP.” Is NY UCS currently utilizing all FedRAMP SaaS offerings for the technology stack including Splunk Cloud SaaS offering, CrowdStrike, Tenable.io, and Qualys?

   ***UCS Response**: Splunk and Tenable are on premises. Qualys and Crowdstrike are hosted in a FedRAMP-compliant GovCloud solution. Per Mandatory Requirement # 3 in the RFP (see page 30), the proposed solution must comply with FedRAMP Moderate or High Impact Level Security Controls Baseline Requirements.*

9. Will the bidder be provided administrative access to configure “UCS Software and Environment” elements in accordance with any current change management processes?

   ***UCS Response**: The Vendor will be given admin rights in its Splunk instance and it will have to follow UCS change management processes.*

10. Are there documentation requirements in place for remediation timelines or is the expectation for [Vendor] to develop baseline documentation?

    ***UCS Response**: Please see page 51 of the RFP for service level requirements. The selected vendor is expected to create the documentation referenced in the question.*

11. Does UCS maintain a staff Information System Security Officer (ISSO) or Information System Security Manager (ISSM) currently that the [Vendor] recommended ISSO will collaborate with directly on vulnerability management and remediation (will affect the implementation phase)?

    ***UCS Response**: Yes, UCS has a Chief Information Security Officer (CISO) and Deputy CISO that will collaborate with awarded contractor.*

12. Is the current environment accredited and/or authorized and if applicable, to what level and by what accrediting body/framework?

    ***UCS Response**: UCS follows frameworks for CJIS, FedRAMP, and NIST, among others. Upon request, the selected vendor will be provided with information about UCS accreditations.*

13. Does UCS maintain a current System Security Plan (SSP) that clearly defines the extent of the UCS boundary?

    ***UCS Response**: UCS has a cybersecurity plan. At this time, UCS declines to furnish information about its SSP.*

14. Section 5.2 of the RFP outlines the ‘Statement of Work’ for the SOC solution and lists various data sources. Are the sources documented to include mapping to

MITRE and/or any other framework or has UCS determined a framework to map source ingestion to cover gaps based on best practices?

***UCS Response*: UCS maps to MITRE frameworks, among others. The selected vendor will be expected to map alerts to MITRE and other frameworks.**

15. If documentation exists, what is the overall percentage of completion for gap coverage?

***UCS Response*: The selected vendor is expected to address this in its documentation.**

16. Does NY UCS currently own the Splunk licensing for Core, ES, and SOAR? If so, is running in the cloud or UCS hosted environment?

***UCS Response*: UCS has licenses for Splunk Core, Splunk Enterprise Security (Splunk ES) and Splunk Security Orchestration, Automation, and Response (Splunk SOAR). All data remains on premises in a UCS-hosted environment.**

17. Will this licensing be made available to the SOC provider to avoid redundant costs?

***UCS Response*: UCS will dedicate a Splunk instance to the selected vendor.**

18. Section 5.2 ‘Statement of Work’ notes UCS is utilizing Splunk Security Orchestration Automation and Response (SOAR) and Section 5.1 ‘Current State’ notes “must operate within the UCS Software and Environment” resulting in licensing being dependent on UCS. How many licenses/users will be provided for the SOC solution, or will the SOC solution be dependent on UCS SOAR Engineers to develop automation and tune alerts based on bidder advice and guidance?

***UCS Response*: The Awarded Contractor will be responsible for developing automation and tuning alerts within awarded contractor’s instance of Splunk, which UCS will provide. Awarded contractor must have a Splunk engineer and a SOC team to create automation and alerting within the UCS environment.**

19. Section 5.1 ‘Current State’ includes a list of technologies. What modules and services were included in the Qualys procurement such as Vulnerability Management, Detection, and Response, Cloud Agent, Qualys PCI, Threat

Protection, Continuous Monitoring, Patch Detection, Cloud Agent, Cloud Inventory, and/or additional modules not listed herein?

<u>UCS Response</u>: Provision of this information is not relevant to the bid response, therefore UCS declines to furnish information about modules and services purchased through a separate procurement.

20. What will be included for scanning and what level of scanning is currently being provided via Qualys?

    <u>UCS Response</u>: The selected vendor will not be performing scanning. The vendor will be creating alerts and responding to incidents as well as creating automation using with the Splunk SOAR. The selected vendor will be expected to correlate vulnerabilities with incidents.

21. Exhibit F - Security Operations Center Terms and Conditions requires “Host all UCS metadata.” If data is unable to leave the UCS premise based on mandatory requirements, how is the bidder able to extract the metadata to host accordingly?

    <u>UCS Response</u>: Per page 9 of the RFP, “Data, including event logs and network flow data, remains on UCS premises and does not leave the UCS environment; however, metadata regarding security alerts may be entered into the selected contractor’s ticketing system.” The only metadata that will leave the UCS environment is ticket information in Jira (and only certain field of that information will be available).

22. Exhibit E; App A; and/or Exhibit F - What are the caps on limited liability and consequential damages?

    <u>UCS Response</u>: UCS will entertain contract language that clarifies the indemnity and warranty language in Exhibit E to reasonably allocate risk among the parties. Please note that any such language must adhere to the general indemnity/warranty provisions in the RFP and be approved by NYS Office of Attorney General and OSC.

Vendor # 9

<u>Questions:</u>

1. RFP Section - DOCUMENT ENCLOSURE CHECKLIST - RFP Text - "UCS Request for Bid/Proposal Form DOCUMENT ENCLOSURE CHECKLIST Contractor Certification to Covered Agency (Form ST-220-CA) EXHIBIT C: CONTRACTOR CERTIFICATION OF MINIMUM BIDDER QUALIFICATIONS

AND MANDATORY REQUIREMENTS - QUESTION - Can you please advise where bidders should include these four forms in our proposal response?

<u>UCS Response</u>: These forms may follow the copies of bidder's certificates of insurance or other adequate proof evidencing the insurance coverages required by the bid specifications.

2. We did not find them listed in RFP sections 6.2, 6.3, or 6.4. Should we include them with the "Required Proposal Documents" or "Additional Bid Documents"?

   <u>UCS Response</u>: The requirement for Form ST-220-CA and a link to that form appear on page 45 of the RFP. The Contractor Certification of Minimum Bidder Qualifications and Mandatory Requirements appears in Exhibit C on pages 30–31. The various documents that constitute the "Required Proposal Documents" and "Additional Bid Documents" do not need to be segregated from one another; all such documents may be furnished together. Ideally, the order in which such documents are provided follows the order in which those documents are listed in the Document Enclosure Checklist, but that ordering it not a requirement.

3. RFP Section -VI. BID RESPONSE DOCUMENTS, 6.2.2 Responses to Exhibit D – Technical Components Proposal and Weighting - RFP Text - The narrative should not exceed 25 pages. QUESTION - Will NYS OCA consider expanding the page limit to 50 pages given that the individual component requirements in Exhibit D exceed four pages?

   <u>UCS Response</u>: As stated on page 17 of the RFP, "The narrative should not exceed 25 pages. References are not included in this page limit." Please note that a vendor may structure one response to respond to more than one Component.

4. RFP Section - II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS - RFP Text - The proposed solution must supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment; - QUESTION - Will the Splunk engineer be on site or remote? If required to be onsite, where will they be located?

   <u>UCS Response</u>: The Splunk engineer does not need to be on site, but that individual must be located in the United States while working pursuant to the contract resulting from this RFP. See Component # B3 on page 34 of the RFP, which states, "Bidder will ensure that employees or subcontractors assigned to the UCS account will be located physically in the continental United States when delivering SOC services."

5. RFP Section - II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS - RFP Text - Mandatory Requirement 3 - QUESTION - Is the

requirement for the platform and vendor to be FedRamp certified or FedRamp compliant?

<u>UCS Response</u>: The proposed solution must be FedRAMP complaint. See, for example, page 15 of the RFP ("When evaluating whether the proposed solution is FedRAMP compliant, preference will be given to security controls that comply with High Impact Level Security Controls Baseline.").

6. Our platform is not a system of record and any CUI will be retained in customer technologies or FedRAMP compliant solutions meeting the needs. For specific requirements in meeting FedRAMP moderate & high, we may accommodate the US-domestic monitoring needs. Is this acceptable for meeting the requirement minimum qualification?

   <u>UCS Response</u>: Determinations regarding the adequacy of a bidder's proposal are only made upon receipt of a bidder's proposal. UCS will not speculate in a Q&A document whether a hypothetical or a characterization of a bidder's attributes satisfies a minimum qualification.

7. RFP Section - II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS - RFP Text - Mandatory Requirement 8 - QUESTION - Do you require a dedicated Splunk engineer for your requirement, or if it is acceptable to have a team of engineers assigned and generally you will have the same engineer since they will have the most familiarity?

   <u>UCS Response</u>: Per Mandatory Requirement # 8 as shown on page 4 of the RFP, "The proposed solution must supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment." See also page 12 of the RFP. Bidders may propose to supply more than one such engineer, but it is a minimum requirement to supply at least one such engineer.

8. RFP Section - II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS - RFP Text - Mandatory Requirement 2 - QUESTION - Log metadata (not just alert metadata) is brought into the our SaaS based platform for data stitching and threat hunting as part of investigations and is kept within the continental US. This data is not retained post-investigation and all data remains within the UCS Splunk instance for permanent storage. Is this acceptable?

   <u>UCS Response</u>: No, this is not acceptable. All UCS Splunk data must stay within the UCS environment and in the UCS ticketing system. The selected vendor is expected to create alerts within the UCS Splunk environment and the UCS Splunk SOAR environment. The only metadata would be certain fields from the UCS Jira ticketing system. No data will leave the UCS environment.

9. RFP Section - II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS - RFP Text - Mandatory Requirement 10 - QUESTION - We do not currently do NIST assessments against our environment as we use other compliances. We primarily use SOC 2 assessments and compliance. Please confirm if this is acceptable or if we should do an internal gap assessment against NIST Tier 4 to be able to show our status?

   <u>UCS Response</u>: Per Mandatory Requirement # 10 as shown on page 4 of the RFP, "The proposed solution must comply with NYS Office of Information Technology Services Security Policy No. NYS-P03-002 (as set forth in Exhibit H), and <u>it must be NIST Tier 4 compliant</u>" (emphasis added). As indicated on page 31 of the RFP, the bidder must certify that its proposed solution is NIST Tier 4 compliant and, as shown in Component # G5 as set forth on page 36 of the RFP, the proposal should describe "the extent to which the proposed solution will monitor, detect, respond, and remediate threats in conformity with standards, guidelines, and best practices of [NIST]."

10. RFP Section - V. SCOPE OF WORK - RFP Text - Scoping - QUESTION - Does UCS also want the proponent to respond to high fidelity alerts from Crowdstrike and provide tuning and detections against this environment?

    <u>UCS Response</u>: The selected vendor's SOC will respond to all alerts, not just CrowdStrike ones. All logs go to UCS Splunk, and the vendor is expected to create all incidents and alerts within the UCS Splunk environment. The selected vendor's SOC will work with the UCS SOC before anything is tuned.

11. RFP Section - V. SCOPE OF WORK - RFP Text - Scoping - QUESTION - How many licenses does UCS have for Crowdstrike?

    <u>UCS Response</u>: UCS has over 30,000 license endpoints.

12. How many are in use currently?

    <u>UCS Response</u>: This information will be supplied to the selected vendor upon request.

13. RFP Section - V. SCOPE OF WORK - RFP Text - Scoping - QUESTION - What Crowdstrike licenses does UCS currently make use of?

    <u>UCS Response</u>: UCS has all modules from Crowdstrike except Falcon Complete.

14. RFP Section - V. SCOPE OF WORK - RFP Text - Scoping - QUESTION - Does UCS currently use the CrowdStrike Falcon Complete Service?

    ***<u>UCS Response</u>*: No, UCS does not currently use the Falcon Complete module.**

15. RFP Text - Automations - QUESTION - What types of activities will UCS like the proponent to perform on their behalf depending on the severity of the alert? For instance, isolation of hosts, disabling/resetting passwords, deleting malicious emails, blocking threat Ips on the firewall, etc.

    ***<u>UCS Response</u>*: The selected vendor will be performing all SOC duties, including reporting on all alerts, working with the UCS staff to tune alerts the vendor has created, disabling/resetting passwords, deleting malicious emails, blocking threat IPs on the firewall, etc. All of this will be done using Splunk SOAR, which the vendor will create, with notification to the UCS SOC. Dedicated vendor SOC analysts are expected to work all incidents.**

16. RFP Text - Detections - QUESTION - Our default methodology for detections it to perform the detections directly against the UCS Splunk environment via correlation APIs, which means a significantly faster rollout of our detections and faster time to value. Is this an acceptable method for performing detections?

    ***<u>UCS Response</u>*: No, the selected vendor must use the UCS instance of Splunk and Splunk SOAR. No data will leave the UCS environment.**

17. RFP Text - Connectivity - QUESTION - A VPN will be required for access/connectivity from our datacenters to yours to access the UCS Splunk for maintenance, monitoring, API connectivity, etc. Is this acceptable?

    ***<u>UCS Response</u>*: UCS will issue a dedicated VPN to the vendor to configure the Splunk instance, but no API connection will be allowed to the vendor. The vendor will strictly work in the UCS Splunk instance creating all alerts and incidents.**

18. RFP Section - RFP Exhibit A - Pricing Sheet - RFP Text - Do not otherwise alter this Pricing Sheet in any manner. Any changes, deletions, or additions to the Pricing Sheet (other than in fields highlighted in yellow) may result in rejection of the bid response. - QUESTION - If bidders wish to propose optional services, how should we incorporate the pricing for any optional services in RFP Exhibit A?

    ***<u>UCS Response</u>*: UCS is only soliciting those services specified in the RFP. Bidders should refrain from proposing optional services. The pricing for any services that the bidder proposes to provide should be included either as “one-time onboarding costs” or “security operations center (SOC) services,” and UCS will not exclude certain amounts designated “optional” in a bidder’s proposal. All pricing furnished on the Exhibit A – Pricing**

Sheet will be considered when assigning cost points per Section 3.2.2. as set forth on page 7 of the RFP.

Vendor # 10

Questions:

1. Section - 1.1 Purpose and Scope - QUESTION - Vulnerability Management and Remediation is referenced as in scope for this project and evaluation. Is it UCS's intention that the selected vendor will assume responsibility for managing the existing Qualys and Tenable.SC environments and corresponding Vulnerability Management Program or does this reference the ability to use and monitor the data coming from those tools within the Splunk/SOC environment?

   ***UCS Response**: The selected vendor will not manage the existing vulnerability tools. Instead, the vendor will only correlate alerts to vulnerabilities within UCS where applicable. The selected vendor will monitor the vulnerability data within Splunk.*

2. Section - Mandatory Requirement 3 - QUESTION - Is FedRAMP authorization a requirement or will other controls such as SOC2 / SOC 3 / PCI DSS / etc suffice?

   ***UCS Response**: As indicated in Article II of the RFP: "The proposed solution must comply with Systems and Organization Controls 2 (SOC 2®) requirements" and "[t]he 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.*

3. If FedRAMP is in fact perceived as a requirement, can you please explain the reasoning for this?

   ***UCS Response**: FedRAMP compliance standardizes security assessment and authorization for cloud products, and it is standardized approach to security assessment authorization as well as continuous monitoring for cloud products and services.*

4. Mandatory Requirement 6 - QUESTION - Can UCS please define what your criteria is for determining what a "SOC Level 1", "SOC Level 2", and "SOC Level 3" analyst is?

   ***UCS Response**: SOC Level 1 - Most duties involve security monitoring for suspicious activity and possible threats. Analysts at this level are not often involved in combating threats. Instead, if a Tier 1 analyst believes something needs a closer look, that person will create a ticket and pass it to a Tier 2 analyst for review.*

SOC Level 2 – Analysts at this level are more experienced than Tier 1 analysts. They can do everything a Tier 1 analyst can do if needed, but their main job is to dive deeper into issues referred to them by Tier 1 analysts. While investigating an issue, a Tier 2 professional will gather more data from various sources for further investigation. The Tier 2 professional will also try to find where the threat came from and how it breached the system to prepare an adequate response.

SOC Level 3 – Analysts at this level are at the top of the analyst hierarchy. These highly experienced professionals employ their advanced skill sets to support Tier 2 analyst responses to complex security issues. Additionally, Tier 3 analysts are threat hunters. They routinely look for threats that may have slid past a firm's defenses — along with any vulnerabilities those threats may have exploited to breach a system.

If the vendor has the similar analysts but with different terms or titles, please explain.

5. Section - Mandatory Requirement 8 - QUESTION - Is it UCS's expectation that you will have access to a named Splunk engineer 24x7x365 to create custom searches and perform platform upgrades as needed?

   UCS Response: No, UCS does not expect to have access to a named engineer 24x7x365, but the engineer should be actively working on creating, updating, and tuning alerts as needed. It will not be satisfactory for UCS to wait weeks to have new alerts created or even multiple days for something to be implemented within the UCS environment. If an alert needs tuning, the Splunk engineer should be actively working within the UCS Splunk environment to fix alerting. If there is a disruption to monitoring or alerting off hours and the Splunk reporting stops working, the vendor should have the Splunk engineer available immediately to fix or update an alert if deemed critical. Although UCS does not expect a Splunk engineer to be available at all times working on routine matters, the selected vendor must supply SOC analysts working 24x7x365 days a year within the UCS Splunk environment.

6. Section - Mandatory Requirement 9 - QUESTION - Is UCS's intention of this requirement to state that no additional applications, programs, or other software is to be installed on UCS systems for the purposes of log collection and automated response or containment activities?

   UCS Response: As stated in Mandatory Requirement # 9 on page 4 of the RFP, "The proposed solution must not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS." The selected vendor will use and work within the UCS Splunk and the UCS Splunk SOAR environment to create alerting and automation.

7. Section - 5.1 Current State - QUESTION - Can UCS please provide which modules or licenses you currently leverage from Splunk and the corresponding licensing information?

   ***UCS Response*: UCS has licenses for Splunk Core, Splunk Enterprise Security (Splunk ES) and Splunk Security Orchestration, Automation, and Response (Splunk SOAR). UCS maintains the cost of the licenses and has enough licenses for its current workforce. UCS will dedicate a Splunk instance to the selected vendor.**

8. Also can UCS please provide Splunk architecture information or an architecture diagram showing how Splunk is currently deployed?

   ***UCS Response*: For security purposes, UCS will not furnish the requested diagram in a public-facing document; however, this information will be furnished to the selected vendor upon request and, if required prior to contract execution, completion of a non-disclosure agreement acceptable to UCS in its sole discretion.**

9. Section - 5.1 Current State - QUESTION - Does UCS require the integration with UCS's ticketing system (Jira) be a bi-direction integration?

   ***UCS Response*: Integration between the proposed solution and UCS's ticketing system may be bidirectional, but it does not have to be bidirectional.**

10. Section - 5.1 Current State - QUESTION - Can UCS please provide which modules or licenses you currently leverage from Crowdstrike and also the license counts associated?

    ***UCS Response*: UCS has all modules except the Falcon Complete, and there are over 30,000 endpoints.**

Vendor # 11

Questions:

1. What threat intelligence feeds are integrated with UCS's current Splunk environment?

   ***UCS Response*: UCS requires the selected vendor to incorporate alerts from the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Federal Bureau of Investigation, among other sources.**

2. Does UCS expect the vender to integrate additional threat intelligence feeds with the Splunk environment, and if so, how many and at what frequency?

   ***UCS Response*: Yes, it is the expectation of the UCS to integrate additional intelligence feeds. The quantity and frequency will be discussed with the AC during onboarding, and in response to evolving conditions throughout awarded contract term.**

3. Is the "mirrored Splunk Environment" mentioned in Exhibit F.1.E also on-prem, and does it have an identical configuration to UCS's current production environment?

   ***UCS Response*: It is on premises and it has the same logs as the UCS current production environment. The awarded contractor will be responsible for configuring the "mirrored" UCS Splunk environment.**

4. What is the current volume of alerts and Jira tickets produced on a daily/weekly/monthly/annual basis?

   ***UCS Response*: UCS routinely receives over 200 incidents weekly.**

5. How many use cases are enabled and expected to be tuned within the SIEM?

   ***UCS Response*: Currently, there are approximately thirty use cases enabled. The volume of "expected" use cases will be based upon evolving conditions throughout the term of the awarded contract.**

6. Given that UCS's current solution is on-prem, what additional SOC 2 certification is required from the vendor?

   ***UCS Response*: Formal SOC 2 certification is required. 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.**

7. How many new use cases does UCS envision to be deployed on a monthly/quarterly basis?

   ***UCS Response*: The volume of "expected" use cases will be based upon evolving conditions throughout the term of the awarded contract.**

Vendor # 12

Questions:

1. How is Splunk deployed today? On prem, Cloud (AWS, Azure, GCP), Splunk Cloud or Splunk Gov Cloud?

   ***UCS Response*: Splunk deployment is on premises.**

2. In addition to Splunk Enterprise and SOAR, is Splunk Enterprise Security deployed?

   ***UCS Response*: Yes, on premises.**

3. What SIEM or MDR is NYS Courts using today? (Splunk ES or another SIEM)

   ***UCS Response*: UCS is using Splunk.**

4. Who did NYS Courts purchase the current solution from?

   ***UCS Response*: ePlus Technologies, Inc.**

5. What is the scope of the FEDRamp requirement in relation to hosting and managing?

   ***UCS Response*: To clarify, "hosting" is not a requirement of this procurement. "Managing" of the awarded contractor's Splunk instance is a requirement of this procurement. 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.**

6. Can a SOC provider be in the FedRamp certification process during the RFP period?

   ***UCS Response*: Yes, however Awarded Contractor's solution must be FedRAMP compliant at time of contract execution. 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.**

7. Is FedRamp compliance a hard requirement if all of the FedRamp controls can be shown to be in place with an assessment? A self assessment and attestation?

   UCS Response*: Awarded contractor's solution must be FedRAMP compliant. 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.

8. If on site sensors are part of the solution should professional services for installation be part of the response or would NYS Courts install them?

   UCS Response*: The proposed solution must not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS

Vendor # 13

Questions:

1. For a technology platform that is FedRamp in process for approval would it suffice where it meets the baseline controls?

   UCS Response*: Yes, however Awarded Contractor's solution must be FedRAMP compliant at time of contract execution. 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.

2. To receive logs from the various syslog-based data sources (e.g., firewalls/IDS/IPS), a "Data Collector" must be deployed. Is the installation of a virtual appliance acceptable to securely receive and process the log data to ensure encrypted?

   UCS Response*: The proposed solution must not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS.

3. If additional Splunk or similar forwarders are required would UCS add or install?

   <u>UCS Response</u>: The proposed solution must not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS.

4. Are employees that have undergone extensive background checks with Europe Union acceptable to deliver service as part of a 24x7 "follow the sun" model, referencing comments on Staffing 5.3 of page 12 of RFP related to all employees assigned reside within the continental United States.

   <u>UCS Response</u>: As set forth on page 12 of the RFP, "All employees assigned to the UCS account must be physically located in the continental United States."

5. "Level 1, 2, 3 Analysts" were referenced. Can you provide differentiation of responsibilities between each of these?

   <u>UCS Response</u>:

   SOC Level 1 - Most duties involve security monitoring for suspicious activity and possible threats. Analysts at this level are not often involved in combating threats. Instead, if a Tier 1 analyst believes something needs a closer look, that person will create a ticket and pass it to a Tier 2 analyst for review.

   SOC Level 2 – Analysts at this level are more experienced than Tier 1 analysts. They can do everything a Tier 1 analyst can do if needed, but their main job is to dive deeper into issues referred to them by Tier 1 analysts. While investigating an issue, a Tier 2 professional will gather more data from various sources for further investigation. The Tier 2 professional will also try to find where the threat came from and how it breached the system to prepare an adequate response.

   SOC Level 3 – Analysts at this level are at the top of the analyst hierarchy. These highly experienced professionals employ their advanced skill sets to support Tier 2 analyst responses to complex security issues. Additionally, Tier 3 analysts are threat hunters. They routinely look for threats that may have slid past a firm's defenses — along with any vulnerabilities those threats may have exploited to breach a system.

   If the vendor has the similar analysts but with different terms or titles, please explain.

6. If XDR platform solution is FedRamp approved and current endpoint agent utilized within UCS Court Systems is deployed along with all data remaining within their existing tenant will that meet the UCS NY Court Systems FedRamp

requirement with SOC 24x7 services based in USA to support and manage the solution?

<u>UCS Response</u>: Compliance is the requirement. 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.

7. Current Splunk license is 600 GB/day, what is the average amount of data sent to the Splunk SIEM to date each day within the 600 GB/day limit?

   <u>UCS Response</u>: Information about the volume of data sent to the UCS Splunk SIEM is not readily available.

   a. Is the Splunk SIEM on premise or in the Splunk Enterprise Cloud?

   <u>UCS Response</u>: Splunk is on premises.

8. For the FedRamp Certification requirement, Does the Bidder/Vendor have to be FedRamp Certified, or can a Bidder/Vendor's Partner be FedRamp Certified to satisfy this requirement?

   <u>UCS Response</u>: The entity providing the SOC services must be FedRamp compliant. For example, if the prime contractor will subcontract with a separate entity, and that entity will provide all of the SOC services, only the subcontractor must demonstrate compliance.

Vendor # 14

<u>Questions:</u>

1. What is the makeup of the firewall environment?

   <u>UCS Response</u>: All logs for all firewalls go to Splunk. UCS has multiple different firewalls. Additional information regarding the composition of the UCS firewall environment will be provided to the selected vendor.

2. How many of each type of firewall device is in the environment?

   <u>UCS Response</u>: UCS has multiple different firewalls. The selected vendor will use the existing UCS Splunk and Splunk Security Orchestration, Automation, and Response (SOAR). UCS will not install any new software or hardware at the request of the selected vendor to change its current firewall environment. Additional information regarding the composition of the UCS firewall environment will be provided to the selected vendor.

3. How many domains does the environment have?

   ***UCS Response*: UCS will not furnish the information in a public-facing document for security purposes; however, this information will be furnished to the selected vendor upon request and, if required prior to contract execution, completion of a non-disclosure agreement acceptable to UCS in its sole discretion.**

4. How many EDR instances are there and what are they?

   ***UCS Response*: UCS has over 30,000 endpoints on its Endpoint Detection and Response (EDR). Logs from all EDR instances go to the UCS Splunk. The selected vendor will create all alerts from Splunk and automating detections.**

Vendor # 15

Questions:

1. Can the UCS provide a description or inventory of the current UCS software and environment to respondents prior to proposal submittal? As started in the RFP, we understand that this may change. Even a high-level or partial documentation of the software and environment would help

   ***UCS Response*: A description of the current UCS software and environment is available in Section 5.1 beginning on page 8 of the RFP. UCS has over 30,000 endpoints on its Endpoint Detection and Response (EDR). Logs from all EDR instances go to the UCS Splunk. The selected vendor will create all alerts from Splunk and automating detections.**

2. Is any onsite work expected? i.e. at a UCS or DoTCR facility or elsewhere? If so, what is the expected work (e.g. select patching) that needs to be accomplished onsite?

   ***UCS Response*: No onsite work is expected.**

3. Is there an incumbent firm that has provided some or all of the services and products requested previously? If so, are they eligible to bid?

   ***UCS Response*: Yes, there is a firm that has provided some or all of the services requested in this RFP. This UCS bid is open to all offerors.**

4. Is there a MBE goal for this project?

   ***UCS Response*: No.**

5. Is MDM (Mobile device management) included?

   ***UCS Response*: No. Mobile device management is outside the scope of this RFP.**

6. Can we provide recommendations vulnerability scanning?

   ***UCS Response*: The selected vendor will not deliver vulnerability scanning services, and such services are outside the scope of this RFP.**

7. Can we include optional tasks, services and / or products that we believe could add value and meet the spirit of the project?

   ***UCS Response*: UCS is only soliciting those services specified in the RFP. Bidders should refrain from proposing optional services. Bidders should refrain from proposing optional services. The pricing for any services that the bidder proposes to provide should be included either as "one-time onboarding costs" or "security operations center (SOC) services," and UCS will not exclude certain amounts designated "optional" in a bidder's proposal. All pricing furnished on the Exhibit A – Pricing Sheet will be considered when assigning cost points per Section 3.2.2. as set forth on page 7 of the RFP.**

Vendor # 16

Question

Does the MSSP component require FedRamp Compliance given 100% of the solution is On-Premise and under the your Control and we are only assisting with management and activities surrounding the solution?

***UCS Response*: As indicated in Mandatory Requirement #3 in Article II on page 4 of the RFP, "The proposed solution must comply with Federal Risk and Authorization Management Program (FedRAMP®) Moderate or High Impact Level Security Controls Baseline."**