THE PORT OF LOS ANGELES
425 S. Palos Verdes Street Post Office Box 151 San Pedro, CA 90733-0151 TEL 310-SEA-PORT portoflosangeles.org

DATE: February 20, 2025

SUBJECT: REQUEST FOR PROPOSALS FOR CYBERSECURITY ARTIFICIAL INTELLIGENCE IMPLEMENTATION SERVICES:

QUESTIONS AND ANSWERS

FROM: Felicia Ansley, Contract Administrator

Pursuant to the aforementioned Request for Proposals (RFP), all prospective proposers were to submit any questions regarding this RFP by no later than 3:00 p.m. on February 6, 2025. Questions were to be submitted in writing, and all questions and responses were to be posted on the Department's website and www.rampla.org by no later than February 20, 2025.

Below is a list of questions received from prospective proposers, and the Department's responses:

1. **Q: What documentation should we provide with our proposal response to show we are in Los Angeles County and qualify for the 8% [Local Business Enterprise] preference?**

A: The Consultant Description Form, your company's website, and LBE (Harbor) certification status reflected on the company's RAMP profile will all be used by the Contract Administrator to determine if the criteria for the Local Business Preference Program have been met. Prospective proposers may refer to the "Certifications on RAMP" user manual in the Support Section of RAMP (https://www.rampla.org/s/support) for information about adding an LBE (Harbor) certification to their RAMP profile.

2. **Q: I was reviewing your RFP, but don't see any functionality spreadsheet included. Am I missing something or isn't there one that needs to be completed by vendors?**

A: Please refer to Section 3.6, "Checklist for RFP Submittal Requirements" for the elements and documents that must be included within your proposal. A functionality spreadsheet was not mentioned or requested in the RFP.

3. **Q: To assist with providing pricing in the proposal, what is the size of your environment (total average throughput)?**

A: Please refer to Question 54.

4. **Q: As the RFP leaves various approaches to the work open, will it be acceptable if we provide our "Cost" response to reflect more than one approach/scenario? By that I mean we may want to provide more than one Cost response, each reflecting different approaches to the work.**

A: Proposers should outline their best solution to meet the requirements stated in the RFP.

5. **Q: Are there specific systems we need to ensure compatibility with?**

A: As of right now, our systems are very robust. Please propose the type of solution that you are planning to submit. Most of our systems are working in terms of compatibility.

6. **Q: What is the timeline from the date of award to implementation?**

A: That is for you to propose. We want you to provide an approach for the implementation, as well as the schedule for the implementation. We will review your schedule and project implementation approach and that will be one of the factors considered as part of the evaluation. Once a contract is awarded, the schedule can be reviewed accordingly, and a baseline schedule can be established for implementation.

7. **Q: Does the Port of LA need any external monitoring/response as part of this RFP? In other words, do you need outsourced security operations or outsourced SOC services to either augment the Port's existing SOC or allow for 24/7/365 coverage? [Our company] would be interested in augmenting the Port's existing SOC, along with offering our ensemble of AI and ML engines for detection, investigation, and incident response automation.**

A: We are not looking for outsourced security operations as part of this RFP.

8. **Q: In the RFP a "turn-key solutions" is asked for while asking for ability to feed information into an LLM [Large Language Model]. Is the organization prepared to take proposals for solutions that have customs code integrated?**

A: We welcome the use of custom code to suit the needs identified in this RFP.

9. **Q: With regard to Certified Software... whatever solution we are proposing, is there a process or certification internal that we have to be aware of?**

A: We are ISO 27001 certified and adhere to the framework. When it comes to programing code, there are other frameworks and standards. We recommend applying best practices for those coding methods, but in terms of security we will align with that process to ensure that when it becomes operational the ISO 27001 framework will be applied.

10. **Q: What will be the budget for the project or the estimated value?**

A: As stated in Section 1.1 of the RFP, “The budget for this project will not be disclosed”. Section 3.5.7 of the RFP also states, “**The budget for this project will <u>not</u> be disclosed.** Proposers are expected to present their pricing and cost information based on their solution for the needs described in Section 2.2, “Project Scope of Work”.

11. Q: How many tools, machines, different clouds [etc.] will be involved in the aggregation of logs into the proposed solution?

A: We use firewalls, intrusion detection/prevention systems, endpoint security, SIEM, servers, network routers switches and many more. We expect this new solution to be able to analyze all these logs and events.

12. Q: Can you provide more details about the existing SIEM environment including the volume and types of logs?

A: Please refer to Question 54**.**

13. Q: Can the solution team [be comprised of] offshore resources, or [do] they have to be onshore resources only?

A: Please refer to Section 2.2 of the RFP, “Project Scope of Work”. It explicitly states, “The Information Technology Division expects to contract only with firms whose main office/headquarters is based in the United States; <u>offshore resources will not be considered</u>.” A mix of both onshore and offshore resources will also <u>not</u> be considered.

14. Q: What types of data and logs sources (e.g., endpoint, network, cloud) will need to be ingested by the AI solution?

A: Please refer to Question 54.

15. Q: Will you be publishing any types of compatibility interfaces and types (REST/SOAP/Storage bus) for existing systems interoperability?

A: No, we will not.

16. Q: Do you have an estimate of the amount of data you plan to ingest, and how long do you intend to retain it?

A: Data varies depending on the time and date of the logs but assume a large amount of data and a significant retention period. The Harbor Department plans to retain data for a minimum of thirty (30) days.

17. Q: We need a list of all tools that are in place and what data feeds are being ingested.

A: As stated in Section 2.2, “Project Scope of Work”, due to the sensitivity and confidentiality of cybersecurity operations, network diagrams/topology and security technologies will not be provided in this RFP. Technologies utilized are mainly commercial off the shelf solutions that are enterprise grade with minimal source code customization. The Harbor Department will not provide specific details regarding all tools. Please refer to Question 54 for information regarding tools that can be disclosed at this time.

18. Q: Can you please share which EDR, IDS/IPS, firewalls, and other security platforms are currently in place?

A: No, we will not be disclosing that information at this time.

19. Q: Is the goal to replace your existing SIEM or can we add an AI to enhance or augment your SIEM?

A: Please refer to Section 2.1 of the RFP, “Project Goals and Objectives”. The Harbor Department is open to ideas and proposed solutions regarding the augmentation and/or replacement of existing technologies.

20. Q: Is the expectation for client references [that they] must be [from the] government sector? Will private sector client refences be considered?

A: Yes, private sector references will be considered, but government sector references are preferred.

21. Q: We contacted several insurance companies and none will provide the [insurance verification letter suggested in the RFP documents], as they do not do that. Please describe the specific requirement and how other vendors are working through and meeting this requirement.

A: Please refer to Amendment 2 of the RFP.

22. Q: Any limitations on SaaS based solutions vs on-prem as options for technology replacement?

A: We do not foresee any limitations. The proposer should discuss a solution that would meet the goals, objectives, and scope of work discussed in the RFP.

23. Q: Does the solution need to be implemented on premise or will dedicated public cloud solutions, properly secured, meet the requirements?

A: We are open to your proposed solution.

24. Q: Any special requirements for [a] dashboard?

A: Please refer to Section 2.2. of the RFP, “Project Scope of Work”, for the project requirements.

25. Q: Are the event logs stored on premise or in the cloud? If in the cloud, which CSP?

A: Current logs are stored on premises.

26. Q: What level of ongoing support do you expect – 24/7 coverage, on-call or business-hours only?

A: Only technical support coverage is expected for the proposed solution. 24/7 coverage is preferred. No professional services or managed services are required after project completion and transition to the Harbor Department.

27. Q: Will you be looking to replace any of your networking hardware as part of this RFP?

A: No, the intent is to not replace any existing networking hardware. We are focused on the security and the A.I. solution, but if your proposed solution includes hardware replacement, we will take that into consideration.

28. Q: Why can't you disclose the name of your SIEM?

A: Please refer to Question 17.

29. Q: Section 2.2.2 line 13 of the RFP says, "Ability to perform authorization, authentication and accounting." We understand authorization and authentication, but accounting can mean a couple of different things. Can you define what your understanding of accounting is?

A: Accounting would be system logs that are being generated by various platforms like network devices, servers, security devices, endpoint devices, and devices that are operational/informational technologies that are connected to the network. System logs generated are sent to our SIEM platform.

30. Q: Are you planning to use [an] off the shelf A.I. solution (like AWS and Microsoft solution) or would you like to build a new A.I./M.L. model using existing data on LLMs?

A: There is no preference. Please propose what is appropriate for your solution.

31. Q: Is there a maximum number of references allowed?

A: Section 3.5.2 "Firm Qualifications, Experience and References" states that proposals must include "at least three client references". A maximum number is not stated. However, we prefer to limit references to no more than five (5).

32. Q: Is the existing SIEM hosted on-prem (legacy) or is [it] a cloud native SIEM?

A: It is currently on premises.

33. Q: Are you open to using an existing A.I. Agents for SOC product or are you expecting a custom-built solution?

A: We are open to any proposed solution.

34. Q: Being that there are no specific volumes, interface types, [or] data formats [being made available at the proposal stage], is the organization prepared for cost and estimate changes once this information becomes available?

A: No, this is not a "time and materials" contract. There will be a "fixed price" contract executed between the Harbor Department and the selected consultant. However, once a selection has been made, there will be an opportunity to enter into contract negotiations with the selected consultant. During those negotiations, more in-depth discussions can take place, and a final fixed price for the solution will be determined.

Proposers should not assume that once contract negotiations begin that they can introduce significant price increases from what their firm submitted in their written proposal.

35. Q: What is the amount of logs should we expect overall as the sizing of the solution is dependent on that?

A: Please refer to Question 54.

36. Q: Will you consider an early stage startup?

A: Yes, provided all requirements in the Project Scope of Work are met.

37. Q: Will there be any metrics shared today regarding average SOC analyst response time, frequent/manual tasks, or KPIs measured on analysts?

A: No, that will not be shared.

38. Q: Is there a specific LLM [that the] Port of LA has the intention to use?

A: No. The proposer shall recommend an LLM in their proposal.

39. Q: Beyond the 30-day "hot" data, would the expectation be to have searchable, retained etc. data beyond this period?

A: Yes.

40. Q: Do you ingest any external threat feeds in the current solution and does the new solution need to support them?

A: Yes, to both questions.

41. Q: Page 31 of the RFP states that the Harbor Department seeks 25% participation of SBE's, but paragraph 4 contradicts the previous statement by [stating] a 0% requirement. Please clarify how the Harbor will weigh the participation despite a 0% requirement?

A: The top portion of Exhibit B references an overall goal of 25% Small Business Enterprise participation, including 5% Very Small Business Enterprise participation. That goal applies to most professional service and construction contracting opportunities for the Harbor Department. However, in the fourth paragraph on that same page, it states in bold font that "**Based on the work to be performed, it has been determined that the percentage of small business participation will be 0%, including 0% VSBE participation**". That means although there is an overall Harbor Department goal for contracting opportunities, there is a 0% SBE and VSBE participation requirement for this specific project.

Further, Section 3.5.8A of the RFP states that there is not a mandatory Small Business Enterprise or Very Small Business Enterprise requirement for this project (the forms in Exhibit B must still be completed and submitted).

42. Q: Can you speak to the latency requirements between ingestion of your data to insights? Is it in hours/days/minutes/seconds?

A: Everything is sent in real-time. Latency is in milliseconds. The Harbor Department expects this new or augmented solution to provide quick (or the least amount) of latency possible so we can have that information in a timely manner.

43. Q: A.I. Agents for SOC solutions are often interfacing with SIEM/Logs in a similar way that their human analysts were – query and analysis. I'm hearing a lot of discussion of storage/analytics of logs. Are you specifically looking to store and analyze logs outside of your SIEM in this A.I. solution?

A: No.

44. Q: Are there any critical systems or future upgrades planned (e.g., EDR, firewalls, or other network tools) that might be influence how the proposed solution should be accommodate interoperability or scalability?

A: We strive to utilize industry's best technologies and the Cybersecurity Operations Center (CSOC) undergoes continuous technologies refresh. Technologies are upgraded through its life cycle or due to emerging requirements to mitigate cyber risks. The proposed solution shall be interoperable with standard industry tools.

45. Q: You want an A.I. solution that can predict cyber attacks. Is polymorphic malware a concern? How many years of logs data is currently being stored for forensic analysis and forecasting, i.e. 1, 5, 10, 15 years?

A: Yes, polymorphic malware is a concern. The CSOC has been operational for ten years and has investigative data for the past decade.

46. Q: Can you elaborate on the support and maintenance of the network equipment?

A: The selected consultant is only responsible for the maintenance and support of the hardware and software implemented under this project.

47. Q: Do you envision additional capabilities like role-specific dashboards, tailored reports for executives, or natural language queries to maximize adoption?

A: Yes, this solution should have role-based capabilities to allow different tiers of access for executives, management, administrators and analysts. For example, the Chief Information Security Officer will have dashboards different from the Chief Information Officer.

48. Q: Considering the expected growth of digital infrastructure at the Port, do you foresee a need for the A.I. solution to accommodate IoT or operational technology (OT) devices in the future?

A: Yes, please propose if that is within your capabilities.

49. Q: Is the Port of LA utilizing any third party incident response services/retainer?

A: The Cybersecurity Operations Center (CSOC) is managed internally by Harbor Department staff under the Chief Security Information Officer's leadership with support from contractors and consultants that are embedded as part of the team. We will not be disclosing how we structure and strengthen our cybersecurity posture or who our partners are at this time.

50. Q: Are you looking for any security orchestration or automation features as part of the proposed solution? Example: The ability to create automated workflows through playbooks.

A: If it meets the requirements of the RFP, orchestration or automation are welcomed.

51. Q: Can we include optional add-on's to our proposal? Or multiple solution options?

A: Yes, to both questions.

52. Q: The RFP mentions requiring minimal analyst training time. Do you then expect the vendor to stick around and build various types of analyses and operationalize for your team? Or is the expectation that your analysts will migrate to the new tool (assuming its UI is friendly)? Asked in another way, do you expect services beyond implementation?

A: The User Interface of the solution shall be simple, easy to navigate and use without extensive training. The selected consultant shall transfer all intellectual property, licenses, warranty, vendor support and maintenance to the Harbor Department upon completion of implementation.

53. Q: Will you be looking to replace any of your existing security gear (hardware or software tools)?

A: We are open to suggestions.

54. Q: To provide an accurate estimate, additional information would be very helpful. Details such as the volume of logs, the tools in use, specific operating systems, and the extent of custom code needed are critical. If your organization operates in a multi-cloud environment, we would also need to consider the various architectures required, factoring in transfer costs and hybrid connectivity with the on-prem infrastructure that the Port maintains.

Given these complexities, it can be challenging to provide precise quotes without this level of detail. Could you share more about the organization's strategy during this evaluation for ensuring that responses to this RFP align with your specific requirements? This would help vendors deliver solutions that are tailored to your needs.

A: Ingestion of logs fluctuate daily between 60-150 GB. Tools consist of firewalls, routers, switches, servers (Windows and Linux), advanced persistent threat platform, intrusion detection and prevention systems, email security, endpoint detection and response, security information and event management, identity management, and Governance Risk and Compliance platform. The proposer shall recommend custom code for their solution if required.

55. Q: Currently is the Port using physical firewalls? If so how many?

A: Yes, the Harbor Department is using physical firewalls, but the actual number will not be disclosed.

56. Q: Do you have SOAR platform?

A: No.

57. Q: Is there a purchasing vehicle requirement?

A: No, we expect to execute an agreement directly with the selected consultant.

58. Q: Is there an incentive for responding to a small business enterprise?

A: There is no Small Business Enterprise mandatory participation requirement for this project. However, there is a Local Business Enterprise (LBE) preference. Per RFP Section 3.5.8A, proposers who qualify as an LBE will receive an 8% preference on any services valued in excess of $150,000. Proposers who do not qualify as an LBE may receive up to a maximum 5% preference for identifying and utilizing LBE subconsultants. Refer to Exhibit B of the RFP for additional information about what criteria must be met to qualify as an LBE.

59. Q: Do we have to show our subcontractor's rates?

A: It is not a requirement, but it is preferred.

60. Q: Who do you want to respond directly to the RFP, the reseller/partner or the OEM?

A: Any firm who can meet the requirements outlined in the project scope of work (Section 2.2 of the RFP) and who attended the mandatory pre-proposal meeting may respond by submitting a proposal.

61. Q: Curious as to why POLA is not providing proposal points for DVBE (i.e. women owned, disabled veteran owned, native American Indian, etc.)?

A: The Harbor Department's Small Business Enterprise Program does not provide any preference for a Disabled Veteran Business Enterprise or any of the other ownership certifications referenced above. Although we welcome participation from companies that hold those certifications, for this opportunity, preference points will only be awarded for those firms who qualify as a Local Business Enterprise (refer to Question 58) or who utilize subconsultants who are Local Business Enterprises (refer to Question 219).

62. Q: In the section [Project Organization, Personnel] and Staffing, do you require the detailed resumes or just the profiles with the roles and responsibilities?

A: Detailed resumes are recommended. However, please note that all documentation submitted in response to this RFP may become available to the public as a public record and be released without further notification (Section 3.4 of the RFP). Proposers should redact personal information accordingly.

63. Q: Will the decision on the winner be made completely on the submission and pricing or will there be a technical presentation/evaluation phase of the process?

A: Please refer to Section 3.4 of the RFP, "Evaluation Process and Selection Criteria". Please also refer to Exhibit E, "RFP Selection Evaluation Form". Firms will be rated on both their written proposals and interview performance based on those criteria.

64. Q: Will you accept any red-lines that we may make on any of the administrative documents?

A: No. Red-lined administrative documents will cause the entire proposal to be deemed non-responsive. Please carefully read the RFP and the "Tips for a Successful Proposal Submission" supplemental document. Please also refer to Questions 71 and 72.

65. Q: Is Orange County considered local?

A: Yes. Refer to page 2 of the Affidavit of Company Status (Exhibit B of the RFP) for a list of the five counties that are included in the criteria for a Local Business Enterprise.

66. Q: Was there an attendance sheet for this call?

A: Yes, Microsoft Teams automatically created an attendance list for those who logged into the mandatory virtual pre-proposal meeting held on January 23, 2025.

67. Q: Can you provide a list of pre-bid attendees, their company, and their e-mail address? We are a DBE seeking to partner with a prime.

A: The attendance list was published on the Regional Alliance Marketplace for Procurement (RAMP, ID #218092) on January 27, 2025. An updated, more complete version of the attendance list was published on February 6, 2025.

68. Q: [Section] 4.18 [of the RFP mentions] State Tidelands Grants. Is there [a] response or detail we need to include to address this?

A: No. Please refer to Section 3.5 "Proposal Content" and Section 3.6 "Checklist for RFP Submittal Requirements" to see what needs to be included in your proposal. If it is not referenced in those sections, it is not being requested. Section 4.18 "State Tidelands Grants" is part of the Standard Contract

Provisions, which is included in the agreement between the Harbor Department and the selected consultant.

69. Q: If a company has an in-process application to be certified as [a Local Business Enterprise], can we apply as an LBE? Will the Port be willing to sponsor the expediting of an LBE application?

A: If you are referring to an in-process application for LBE-Los Angeles certification, no, the Harbor Department does not sponsor or request expedited review on behalf of any prospective proposers. The relevant certification for this contracting opportunity is LBE-Harbor.

70. Q: Will the Q&A (from this call) be posted sooner than 2/20/25?

A: The Q&A document **may** be posted sooner than February 20th, but proposers should not assume or expect that it **will** be available before that date. We expect to receive a large volume of questions regarding this contracting opportunity, and it will take time for Harbor Department staff to compile them and formulate an official response.

71. Q: If a current Port of Los Angeles vendor is successfully providing services on an existing contract that includes previously agreed upon terms between the Port and the vendor, will POLA consider exceptions to those specific RFP terms that deviate from current signed contracts and prior approved agreements?

A: No, not during the proposal stage. The RFP explicitly states, "**If your firm cannot agree to the following requirements exactly as set forth in this RFP, please do not submit a proposal."**. If your firm is recommended for award, during contract negotiations you may choose to request any exceptions to specific RFP terms at that time. However, there is absolutely no guarantee that those proposed exceptions will be accepted – or even entertained – by the City Attorney preparing the contract, even if those exceptions were accepted for previous/current Harbor Department engagements.

Negotiated terms for previous/current agreements with the Harbor Department do not have any relevance to the requirements stated in the RFP. To be deemed responsive to this RFP, proposers must agree to accept the Standard Contract Provisions **exactly as set forth** in the RFP by submitting a letter stating such (refer to Section 3.5.8D of the RFP).

72. Q: Should those identified exceptions to active and previously agreed upon terms be proposed, is it to be understood that this will result in automatic disqualification of the vendor even if the exceptions listed were previously agreed to by POLA, thus resulting in a no-bid stance from a vendor with extensive proven history with POLA and qualifications directly applicable to this RFP?

A: Yes, that's correct. All proposers who state or propose exceptions to the Standard Contract Provisions in their acceptance letter (Section 3.5.8D of the

RFP) will be deemed non-responsive to that administrative requirement. Please refer to Question 71. There is no preference or exception granted during the proposal stage just because the proposer is an incumbent on a different Harbor Department (or City of Los Angeles) project. Contract terms are negotiated on a project-by-project basis.

73. Q: Could you prioritize your desired 14 features listed in [Section] 2.2.2 of the RFP so that we can properly stage the project? Also, could you list your desired features by stage of project with a timeline?

A: All fourteen features are important. There is no specific order of priority.

74. Q: What current cybersecurity operations and tools are in place at the Port of Los Angeles, such as threat intelligence platforms or incident response systems? (RFP Section 1)

A: Please refer to Question 54.

75. Q: Could you please elaborate on Section 2.2 regarding AI's ability to predict future attacks? What are the Port of Los Angeles's expectations for this type of predictive future attack capability? "Ability to predict historical high-risk incidents, current and future attacks that may affects the Port's digital infrastructure".

A: The proposed AI solution should be able to comprehensively analyze real-time logs, packets, attacks and types, behavior of activities, frequency of activities and output high fidelity information of the next attack on a targeted system(s).

The AI solution should be able to comprehensively analyze historic logs, archived incident cases, historic packets, attacks and types, behavior of activities, frequency of activities and output high fidelity information on potentially compromised targeted system(s).

76. Q: How does the Port currently protect its cloud environments, including Azure, AWS, or other cloud providers? (RFP Section 1)

A: Web Application Firewall, Cloud Access Security Broker solution and/or vendor native security tools.

77. Q: What specific security protocols and procedures are used to mitigate risks in the Port's data centers? (RFP Section 1)

A: The Harbor Department adheres to ISO 27001/27002:2022 standards.

78. Q: What security tools and technologies will be used to support the Port's cybersecurity posture, such as threat detection systems or intrusion prevention systems? (RFP Section 3)

A: Please refer to Question 54.

79. Q: Will the Port use any specific security information and event management (SIEM) systems to correlate and analyze security logs? (RFP Section 3)

A: The Harbor Department has an existing SIEM which is used to correlate and analyze logs.

80. Q: How will the Port of Los Angeles utilize artificial intelligence (AI) and machine learning (ML) to enhance its cybersecurity operations? (RFP Section 3)

A: The Proposer shall provide a solution and use cases for utilizing AI and ML to enhance cybersecurity operations.

81. Q: Can you provide quantifiable SOC metrics that AI's contribution should address?

A: No, this information cannot be provided at this time.

82. Q: Are you looking for an AI solution to automate system maintenance and use-case tuning?

A: An AI solution is not used to automate system maintenance, but it could be utilized for use case tuning.

83. Q: How should the AI solution prioritize alerts and reduce analyst fatigue? Do you have any alert volumetrics now, and expected performance after AI integration? Can you provide any SLA if available?

A: An AI solution should categorize priority severity levels with Critical, High, Medium and Low. Volumetrics will be provided when a consultant is selected. No SLA is currently available.

84. Q: The RFP states the solution should "augment and/or replace" existing technologies. Can you provide a list of the current security technologies in use (even without network diagrams)? This will help us assess compatibility and integration needs.

A: Please refer to Question 54.

85. Q: What are the Port's key performance indicators (KPIs) for cybersecurity operations? How will the success of the AI solution be measured (e.g., reduction in incident response time, improved threat detection rates, etc.)?

A: The success criteria for this project should be aligned to RFP Section 2.2.2, “General Design and Functionality”.

86. Q: Will the protected cloud environment be managed by the Port of Los Angeles or will a third-party cloud service provider (CSP) be used? (RFP Section 2)

A: Proposers should include this information as part of their proposal.

87. Q: What specific compliance requirements, such as HIPAA, PCI-DSS, or GDPR, will be applied to the cloud environment? (RFP Section 2 & 4)

A: ISO 27001 and FedRAMP.

88. Q: Will the Port of Los Angeles utilize any specific managed security services (MSS) to support its cloud environment? (RFP Section 2)

A: Please refer to Question 86.

89. Q: Regarding on-premises vs. cloud, what are the Port's preferred options or constraints? Are there any specific cloud providers preferred or disallowed?

A: Proposers should provide the best solution. The Harbor Department does not have a preference for on-premises versus cloud-based solutions, and no cloud providers are preferred or disallowed.

90. Q: Will the Port use any specific cloud migration and transformation frameworks, such as AWS Well-Architected or Azure Well-Architected, to support its cloud environment? (RFP Section 7)

A: Please refer to Question 86.

91. Q: What specific compliance requirements, such as the NIST Cybersecurity Framework or ISO 27001, will be applied to the Port's cybersecurity posture? (RFP Section 4)

A: ISO 27001:2022.

92. Q: How will the Port of Los Angeles ensure that its cloud environment and security operations comply with relevant regulatory requirements? (RFP Section 4 & 7)

A: Details of incident handling will not be disclosed at this time. The Harbor Department is ISO 27001 certified and adheres to ISO standards.

93. Q: Will the Port utilize any specific compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI-DSS), to support its cloud environment? (RFP Section 4)

A: No, PCI-DSS will not be utilized to support the cloud environment

94. Q: Will the Port utilize any specific security assurance frameworks, such as COBIT or ISO 20001, to support its cybersecurity posture? (RFP Section 6)

A: No.

95. Q: How will the Port of Los Angeles respond to security incidents or breaches, including procedures for containment, eradication, and recovery? (RFP Section 5)

A: Please refer to Question 92.

96. Q: What specific incident response plans are in place to address potential security incidents or breaches? (RFP Section 5)

A: Please refer to Question 92.

97. Q: Will the Port utilize any specific security orchestration, automation, and proxy (SOAR) tools to support its incident response efforts? (RFP Section 5)

A: Please refer to Question 92. Additionally, the Harbor Department is open to tools recommended by the proposer to improve incident response efforts.

98. Q: How will the Port of Los Angeles maintain its cybersecurity posture and strategy, including procedures for risk assessment and management? (RFP Section 6)

A: Please refer to Question 92.

99. Q: What specific security controls will be used to protect the Port's cloud environment and data centers, such as encryption or access controls? (RFP Section 6)

A: The selected consultant shall provide appropriate security controls, encryption methods, access control lists and logging to protect the Harbor Department's cloud environment for this project only.

100. Q: What specific assumptions will be made about the Port's cloud environment, including assumptions about data center infrastructure or network connectivity? (RFP Section 7)

A: This question is unclear.

101. Q: How will the Port of Los Angeles ensure that its cloud environment and security operations meet the required standards and best practices? (RFP Section 7)

A: Please refer to Question 92.

102. Q: Can you describe a technical approach to support the Port's cybersecurity posture, including procedures for security architecture and design? (RFP Section 8)

A: The proposer is to provide a technical approach to support the Harbor Department's cybersecurity posture, including procedures for security architecture and design for this project's solution only. Due to sensitivity of information, the current design of existing infrastructure cannot be disclosed.

103. Q: How will your team develop and implement a comprehensive security plan to address the Port's specific vulnerabilities? (RFP Section 8)

A: Please refer to Question 92.

104. Q: Can you describe any specific methodologies or frameworks your team employs to manage risk and ensure compliance with regulatory requirements? (RFP Section 8)

A: Please refer to Question 87.

105. Q: How will your team communicate cybersecurity best practices to Port stakeholders, including procedures for training and awareness? (RFP Section 9)

A: Please refer to Question 92.

106. Q: What specific communication channels will be used to share cybersecurity information with Port stakeholders, such as email or portal-based systems? (RFP Section 9)

A: Please refer to Question 92.

107. Q: Will the Port utilize any specific security awareness training programs, such as phishing simulations or vulnerability scanning tools? (RFP Section 9)

A: This question is not relevant to this project.

108. Q: The RFP mentions "all types of system-generated logs." Can you provide examples of the different log formats and sources? This will help us assess the complexity of the data ingestion process.

A: Logs are generated from technologies listed in Question 54. Please reference Section 2.2.2 of the RFP “General Design and Functionality”, item 1.

109. Q: The RFP mentions "graphical dependencies of communications between various nodes." What level of detail is required in these visualizations?

A: Visualizations vary based on role-based access. For example, technical staff visualizations focus on technical details, where a CISO dashboard provides higher level security posture.

110. Q: Can you provide further details on the "existing technologies" mentioned for API integration? Knowing the specific systems will help us design an appropriate integration strategy.

A: Please refer to Question 54.

111. Q: Regarding LLMs, are there any specific requirements or preferences for the type of LLM (e.g., open-source, proprietary)?

A: Please refer to Question 38.

112. Q: What is the Port's budget range for this project?

A: Please refer to Question 10.

113. Q: Since we have no one owner, how should we respond to the Owner’s Ethnicity and Gender questions within the form? (Exhibit B, pg. 35)

A: If you have multiple owners of the company, you may put the ethnicity and gender information for one of the owners.

114. Q: Does "Award Total" mean our total price? If not, please tell us what would need to be included here? (Exhibit B, pg. 35)

A: Yes, for "Award Total" on the Consultant Description Form (Exhibit B), the Prime Consultant should indicate the total proposed price of their solution. If the Prime will be utilizing subconsultants for this project, list each subconsultant and indicate either a percentage of the total award that they will receive, or indicate an approximate dollar amount of the subcontract.

115. Q: What is the Port's requirement for retaining data? How much live (hot) data is required? How much cold storage is required?

A: Data shall be retained for a minimum of 30 days. The minimum of 30 days applies to live data and cold storage.

116. Q: What is the total amount of aggregate daily data their SIEM is currently ingesting (I recall that we were going to use internal knowledge)

A: Please refer to Question 54.

117. Q: Has the Port identified any automation use cases that they wish to implement?

A: No.

118. Q: How many devices do you have in your environment?

A: We cannot disclose a specific number of devices for this project.

119. Q: How many devices are desktops/laptops?

A: Please refer to Question 118.

120. Q: How many servers do you have in your environment (this includes on-premise and in the cloud)?

A: We cannot disclose the number of servers in our environment.

121. Q: Do you have containers in your environment? If so, how many?

A: We cannot disclose this information.

122. Q: Would you like e-mail protection and telemetry for e-mail to also be included in the scope of this RFP (this can include Google Mail or Microsoft)? If so, how many accounts do you have, and how many mailboxes do you have?

A: No.

123. Q: Would you like network telemetry and protection, i.e. NDR? If so, what is your network throughput?

A: No.

124. Q: Can you clarify what is meant by "no offshore resources"? Can support be offshore and in the US?

A: Offshore means that the firm is not located in the United States. As stated in the RFP, "offshore resources will not be considered". Please also refer to Question 13.

125. Q: Is savings via a multi-year contract of interest? If so, would you prefer 2 year, 3 year or 5 year options? Commitment would be up front but payments may potentially be done in annual interest-free installments.

A: Yes, please provide one, two, and three-year options. However, please note that the agreement resulting from this RFP with the selected consultant will not exceed a three-year term.

126. Q: Is it possible to get a list of pre-proposal [conference] attendees for this RFP? We are a DBE in the state of CA and [are] looking to partner with larger companies.

A: Please refer to Question 67.

127. Q: Can the Port provide more details on their existing cybersecurity infrastructure and any integration challenges with the proposed AI solution?

A: Please refer to Question 17.

128. Q: Are there any legacy systems that the AI solution needs to integrate with? If so, what are the specific compatibility requirements?

A: No.

129. Q: Are there specific AI or cybersecurity platforms currently in use that must be maintained or replaced?

A: No.

130. Q: Will the vendor be responsible for creating new security use-cases, or is the expectation to enhance the existing ones?

A: Existing security use cases are available. The proposer is encouraged to create new and/or enhance existing use cases to align with new AI solution.

131. Q: What specific compliance and regulatory frameworks, aside from ISO 27001:2022, must the AI solution adhere to?

A: Please refer to Question 87.

132. Q: Will the Port provide a secure environment for testing and deployment, or will the vendor need to set up an isolated test environment?

A: The proposer shall provide solutions for testing and deployment.

133. Q: What level of access will the vendor have to sensitive data, and what are the restrictions around data handling and storage?

A: The selected consultant will have access to cybersecurity logs and data. The consultant must comply with City of Los Angeles and Harbor Department policies on data handling and storage.

134. Q: Can the Port specify the encryption standards required for data in motion and at rest?

A: The selected consultant should provide encryption standards for data in motion and at rest with the approval of the Harbor Department.

135. Q: Will there be periodic security audits of the AI implementation, and what will be the vendor's role in those audits?

A: The selected consultant shall expect periodic audits of the AI implementation. The consultant will work closely with the Harbor Department's security team to ensure their implementation meets industry best practices.

136. Q: The RFP mentions that offshore resources will not be considered. Can the Port clarify if remote work is allowed for U.S.-based teams, and under what conditions?

A: As stated in Section 2.2, "The selected Contractor will be expected to be onsite at the Harbor Department's Administration Building at the beginning of the engagement, but tasks can later be performed remotely (with approval from ITD staff).".

137. Q: Will the Port provide its own data scientists and cybersecurity experts to collaborate on tuning the AI models, or is the vendor expected to provide these services?

A: The Harbor Department and the selected consultant shall collaborate to tune the AI models.

138. Q: What is the expected timeline for implementation, and are there any critical milestones the vendor must meet?

A: The expected timeline for completing this implementation shall not to exceed 24 (twenty-four) months. We have not identified any critical milestones at this time.

139. Q: What specific response times and support levels are expected from the vendor in case of cybersecurity incidents?

A: Technical support for handling cybersecurity incidents must be available 24 hours a day, 7 days a week for the duration of the 3 year agreement.

140. Q: Does the Port require a specific Service Level Agreement (SLA) for ongoing AI model updates and maintenance?

A: The Harbor Department does not currently have a specific SLA for AI model and updates and maintenance. The proposer shall provide industry standard SLA recommendations.

141. Q: Is there a budget range that the Port can disclose, even informally, to help vendors align their proposals with expectations?

A: No. Please refer to Question 10.

142. Q: What level of automation is expected from the AI system in reducing analyst workload? Are there any specific benchmarks or automation goals?

A: The selected consultant shall propose and demonstrate new solutions to reduce analyst workload. No specific benchmarks are available at this time.

143. Q: How does the Port prioritize cost vs. capability when evaluating AI solutions?

A: Please refer to Exhibit E, “RFP Selection Evaluation Form”.

144. Q: Will there be additional funding for future enhancements beyond the initial contract term?

A: Additional funding will be determined at a later date.

145. Q: Is the vendor expected to provide cost projections for ongoing maintenance after the initial three-year contract period?

A: No.

146. Q: Will the vendor be responsible for training the Port’s cybersecurity analysts, or will a separate training team handle that?

A: Yes, the selected consultant will be responsible for providing training to the Harbor Department’s cybersecurity analysts.

147. Q: How many personnel will need to be trained, and what level of expertise do they currently have in AI-driven cybersecurity solutions?

A: Up to ten (10) people will need to be trained. The level of expertise of the personnel on AI-driven cybersecurity solutions will not be disclosed.

148. Q: Does the Port require custom training materials, such as interactive modules or hands-on labs, as part of the vendor's deliverables?

A: The selected consultant shall provide training materials on the implemented solution for continuous operations.

149. Q: Is the Port open to a phased rollout of the AI solution, or does it require a full implementation at once?

A: The selected consultant shall provide a full implementation under the agreement resulting from this RFP. The full implementation can be completed in phases provided it is done within 24 (twenty-four) months. Please refer to Section 3.5.6 of the RFP, “Timeline”.

150. Q: How does the Port plan to handle resistance to change among cybersecurity personnel, and what role is expected from the vendor in this transition?

A: The Harbor Department and the selected consultant shall collaborate to ensure knowledge and operations are transitioned smoothly at the end of the agreement.

151. Q: What is the daily volume of logs and events across all systems, and can you provide the number of log-generating sources (e.g., firewalls, servers, endpoints, applications)?

A: Please refer to Question 54.

152. Q: Are there specific data formats (e.g., JSON, syslog, or proprietary formats) that must be ingested, parsed, and normalized?

A: Please refer to Question 54.

153. Q: What is the current Events Per Second (EPS) rate sent to the existing solution, and what is the expected EPS growth over the next 1–3 years?

A: The average EPS is 2500. Expect growth of 20%.

154. Q: Are there existing event correlation rules or thresholds for detecting security incidents? If so, could you provide examples or documentation of the expected logic or scenarios?

A: Yes. Correlation rules include but are not limited to geolocation, privilege access, denial of service, endpoint security, malware activities and more.

155. Q: What role does external threat intelligence play in your operations, and do you use any specific feeds or platforms that must be integrated? What integration method is required (e.g., API)?

A: External threat intelligence is an integral part of cybersecurity operations. API integration is currently used.

156. Q: Are incident response workflows currently documented? If so, can you provide examples or summaries of existing escalation and remediation processes?

A: Yes, incident response workflows are currently documented. Due to the sensitivity of security operations, existing escalation and remediation processes will not be disclosed.

157. Q: Should the solution support the automation of ticket creation and resolution processes? If so, what specific integration points are needed?

A: Automation of ticket creation and resolution processes is preferred but not required.

158. Q: Are there specific auditing and reporting requirements, such as periodic compliance reports or real-time audit trails?

A: The selected consultant's proposed solutions shall have Authentication, Auditing, and Authorization capabilities.

159. Q: What are the documentation requirements for workflows, workbooks, and operational procedures to enable the Port to take ownership of the solution post-implementation?

A: The selected consultant shall provide workflows, workbooks, and operational procedures at the closeout of the project.

160. Q: What specific knowledge transfer and training deliverables are required to prepare Port staff for independent operation and maintenance of the solution?

A: The selected consultant shall provide turnkey knowledge transfer and training of the implemented AI solution to prepare the Harbor Department's staff for independent operation and maintenance at the closeout of this project. Knowledge transfer and training deliverables include, but are not limited to, training sessions, training materials, hardware/software manuals, system design, system configurations and restoration procedures.

161. Q: Are there established use cases or workflows currently utilized by the Port that the implementation team can reference or build upon during the project?

A: Yes. Please refer to Questions 154 and 156.

162. Q: Should the solution enhance or replace any existing use cases? If so, can you provide documentation of the current workflows and their desired outcomes?

A: Please refer to Section 2.2.2 of the RFP "General Design and Functionality", item 11.

163. Q: Are there specific expectations for the ownership of custom-developed workflows, scripts, or system configurations, including intellectual property rights?

A: Please refer to Section 2.2.5 of the RFP, "Project Closeout", for guidance.

164. Q: What is the process for transferring licenses and third-party agreements to the Port at the conclusion of the project?

A: The Harbor Department (Port of Los Angeles) will be the owner of any related licenses at the conclusion of this project.

165. Q: What are the primary objectives for dashboards and reporting (e.g., executive summaries, SOC operational metrics, compliance tracking)?

A: Dashboards and reporting shall provide security posture and efficiency of the solution for various personnel levels.

166. Q: Should the solution support role-based access to different views and reports, and if so, how many unique roles or user types need customization?

A: Yes. The solution should support role-based access to different views and reports. The system should have Root, Super Administrator, Administrator, Read-Only Administrator, Read-Only Analyst, CEO, CIO, CISO, Security Manager, Analysts, and a custom role to create on-demand needs to access the solution.

167. Q: Can you provide the estimated number of endpoints, users, and devices across the infrastructure that must be monitored and managed?

A: Please refer to Questions 54, 118 and 222.

168. Q: Are there specific preferences for deployment models (on-premises, cloud-based, or hybrid) and any restrictions on hosting data?

A: The proposer shall provide cloud, on-premises or hybrid solutions as deemed necessary. Please refer to RFP Section 2.2.1 “Security Requirements and Governance”, item 3.

169. Q: What key performance indicators (KPIs) or success criteria will the Port use to evaluate the solution after implementation?

A: Please refer to Question 85.

170. Q: What are the required service-level agreements (SLAs) for ongoing maintenance, issue resolution, and system availability?

A: Please refer to RFP Section 2.2.3 “Operations” and Section 2.2.2 “Warranty, Maintenance and Support”.

171. Q: Are there custom or legacy applications requiring bespoke integrations? If so, can you outline any known API or connectivity requirements?

A: No.

172. Q: Can you please clarify if the prime’s subcontractors need to be ISO certified or just adhere to the compliance of the certification?

A: The Prime's subcontractors need to adhere to ISO 27001 standards; certification is preferred but is not required.

173. Q: Can you confirm if there is a need for all key personnel to be onsite for the roll out of the project, or just the individuals building the workflows and APIs of the solution?

A: Key personnel are required to be onsite, and supporting members are optional to be onsite for the rollout of this project.

174. Q: How many different roles will need dashboards based on their role?

A: Please refer to Question 166.

175. Q: How many custom developed use-cases does the Port of LA leverage in the existing SIEM and how many of them are considered essential (must have) moving forward?

A: The Harbor Department’s security operations utilize out of the box and custom use cases within the SIEM solution. We are receptive to the enhancement and replacement of existing use cases. Total use cases will not be disclosed but will be provided when the consultant is selected.

176. Q: Does the Port of LA leverage User Behavior Analytics (UBA) features of its existing SIEM?

A: Yes.

177. Q: What [are] the log storage requirements for historical data? What are the short-term (hot) and long-term (cold) log retention requirements for the Port of LA to meet operational and compliance needs for its SIEM and for the Cybersecurity Artificial Intelligence Implementation Services related log data?

A: Please refer to Question 115.

178. Q: How many distinct log source types and their count [are] ingested into the existing Port of LA SIEM? How many of them are ingesting via API integration?

A: Please refer to Question 74. The selected consultant shall account for up to ten (10) APIs for integration.

179. Q: Can the Port provide the daily, weekly, and monthly average Peak Events Per Second (EPS) rate (raw EPS) observed in the Port of LA SIEM?

A: Yes, that information will be provided when a consultant is selected.

180. Q: What is the projected future growth of log volume per week or month?

A: Please refer to Question 153.

181. Q: Does the Port of LA have a Security Orchestration, Automation, and Response (SOAR) capability in place today? If so, how many workflows/playbooks are in use?

A: Please refer to Question 56.

182. Q: Do you have an ITSM platform integrated into the SIEM, or another case management system?

A: Yes. We cannot disclose the specifics of the existing technology implementation at this time.

183. Q: Can the Port provide the list of Applications and its hosted model (Cloud) County to be part of the overall Security implementation and managed services scope?

A: Due to the sensitivity of security operations, a list of applications and its hosted model will not be disclosed. That information will be available after a consultant is selected.

184. Q: Are there documented Cybersecurity, data, and AI policies and procedures in place which are reviewed and updated frequently?

A: Yes.

185. Q: Is there a dedicated cybersecurity team or officer responsible for infrastructure security?

A: Yes.

186. Q: Is cybersecurity integrated into the organization's overall business strategy?

A: Yes.

187. Q: Does the organization comply with relevant cybersecurity regulations and standards and are regular audits conducted to ensure compliance?

A: Yes.

188. Q: Has a comprehensive risk assessment been conducted for the infrastructure and are risks prioritized and mitigated?

A: Yes.

189. Q: Does the organization use threat intelligence to identify and respond to emerging threats and is integrated into the cybersecurity strategy?

A: Yes.

190. Q: Is there a documented and approved incident response plan how often are incident response drills conducted?

A: Yes, but further details about drills cannot be disclosed at this time.

191. Q: Is there an up-to-date inventory of all hardware, software, and network assets and are they based on their criticality to the infrastructure?

A: Yes.

192. Q: Are systems and devices configured according to security best practices and configuration changes tracked and audited?

A: Yes.

193. Q: Are strong authentication methods (e.g., multi-factor authentication) used for accessing critical systems? Are user permissions managed and reviewed?

A: Yes, to both questions.

194. Q: Are privileged accounts (e.g., admin accounts) monitored and controlled with access restrictions to sensitive systems?

A: Yes.

195. Q: Are there policies for granting, reviewing, and revoking access to critical systems?

A: Yes.

196. Q: Are firewalls, intrusion detection/prevention systems (IDS/IPS), and other perimeter defenses in place? Are these systems monitored and updated?

A: Yes, to both questions.

197. Q: Are there measures to protect against common cyber threats like phishing, ransomware, and DDoS attacks?

A: Yes.

198. Q: Is network segmented to limit the spread of potential threats and are segmentation policies enforced?

A: Yes.

199. Q: Are network activities continuously monitored for suspicious behavior?

A: Yes.

200. Q: How long are logs retained, and how are they protected from tampering?

A: The SIEM has at least one copy of logs. Approaches for protection from tampering will not be disclosed.

201. Q: Are all endpoints (e.g., servers, workstations, IoT devices) protected with antivirus and anti-malware software and how often are these protections updated?

A: Yes. Updates are applied at least daily, and some are more frequent depending on criticality of the system.

202. Q: Is there a process for regularly applying security patches and updates? How are vulnerabilities identified and addressed?

A: Yes, there is a process for regularly applying security patches. Vulnerabilities are identified and addressed through our security operations policies and procedures.

203. Q: Is sensitive data encrypted both at rest and in transit? Are there measures in place to protect sensitive information from unauthorized access?

A: Yes, to both questions.

204. Q: Are regular backups performed, and are they securely stored? Is there a tested data recovery plan in place?

A: Yes, regular backups are performed, and data is securely stored. The Harbor Department is ISO 27001 certified, and the data recovery plan conforms with the requirements of the standards.

205. Q: Are physical access controls (e.g., biometric scanners, keycards) in place for critical infrastructure facilities and how are the logs monitored and reviewed?

A: Yes, physical access controls are in place which are monitored and reviewed by the Harbor Department's law enforcement division.

206. Q: Are surveillance systems (e.g., cameras, motion detectors, IoT Sensors) used to monitor critical areas? Are these systems integrated with cybersecurity measures?

A: Yes, to both questions. Surveillance systems are used to monitor critical areas.

207. Q: Are third-party vendors assessed for cybersecurity risks before onboarding and is third-party access to infrastructure systems monitored and controlled?

A: Yes, to both questions.

208. Q: Are supply chain risks identified and mitigated? Are software and hardware components verified for security before deployment?

A: Yes, to both questions.

209. Q: How are cybersecurity incidents detected (e.g., SIEM systems, data-driven analytics)? What is the average time to detect an incident?

A: Please refer to Question 74. Due to the sensitivity of security operations, the average time to detect an incident will not be disclosed.

210. Q: Is there a documented incident response plan? How quickly can the organization respond to and contain an incident?

A: Yes. Due to sensitivity of security operations, response and containment information will not be disclosed.

211. Q: Are business continuity and disaster recovery plans in place? How often are these plans tested and updated?

A: Please refer to Question 204.

212. Q: Are AI and automation tools used to enhance cybersecurity (e.g., threat detection, response automation)? Do enterprise applications use AI, such as HRIS, Financial Systems, Payroll Systems, etc.? How are these tools integrated into existing systems?

A: The selected consultant shall propose AI and automation tools to enhance cybersecurity. Currently, HRIS, Financial Systems, Payroll Systems, etc. are not within scope of this project.

213. Q: If cloud services are used, how are they secured? Are cloud environments regularly audited for compliance and security?

A: Current cloud services have security controls in place. If the question is intended to address this project, then the selected consultant shall propose solutions to safeguard the environment including the data.

214. Q: What KPIs are used to measure the effectiveness of cybersecurity systems? Are these metrics reported to leadership?

A: Please refer to Question 85.

215. Q: How are lessons learned from incidents and audits used to improve cybersecurity? Is there a process for continuous improvement of cybersecurity practices?

A: Please refer to Question 92.

216. Q: Are critical systems designed with redundancy to ensure availability during an attack? How often are failover systems tested?

A: Yes, for its intended purpose. Failover systems are tested frequently.

217. Q: Is there a disaster recovery plan in place for critical infrastructure? How often are disaster recovery drills conducted?

A: Please refer to Question 204.

218. Q: Are vendors expected to identify and create/update any missing cybersecurity processes and procedures or missing compliances?

A: No. The selected consultant shall be responsible for the requirements stated in Section 2.2.2 of this RFP only.

219. Q: We will have a team consisting of a prime and subcontractor(s). I will most likely be the prime. If my local company has less than 50 team members but my subcontractor has a local presence with 50+ [employees], will our team qualify for the 8 points [for a] Local Business Enterprise?

A: Under the Local Business Preference Program, only the prime will receive the full 8 points. However, as stated in the RFP (Section 3.5.8A), "Proposers who do not qualify as a LBE may receive a maximum 5% preference for identifying and utilizing LBE subconsultants."

Per Section 10.47.7B of the Local Business Preference Program Ordinance, "When applying the Local Subcontractor Preference to a Proposal, the score awarded by the Awarding Authority to the Proposal submitted shall be increased by one percent of the total possible evaluation points, up to a maximum of five percent, for every ten percent of the total cost of the proposed work under the contract to be performed by a Local Subcontractor or Local Subcontractors; provided that each Local Subcontractor, the work of the Local Subcontractor and the cost of the work of the Local Subcontractor are specified clearly in the Proposal."

220. Q: Is the pre-bidder's conference mandatory attendance requirement for the prime or can a proposal team member, who is not the prime, participation be acceptable in place of the prime's attendance?

A: The mandatory attendance requirement applies for the prime. Proposals will not be considered from any firm who did not attend the mandatory meeting.

221. Q: Does the 1,000 employees count include contractors?

A: No.

222. Q: What is the total number of users in your environment?

A: Approximately 1,000 Harbor Department users.

223. Q: How many devices do you expect to monitor with this solution?

A: The selected consultant shall provide a plan to monitor various types of devices. Please also refer to Question 118.

224. Q: What is the approximate size of your security operations team?

A: Due to the sensitivity of security operations, the size of the security team will not be disclosed.

225. Q: Do you have an internal security operations team, or is it outsourced to an MSSP/MDR provider?

A: The Harbor Department has a security operations team.

226. Q: Is your infrastructure on-premises, cloud-based, or a hybrid model? If hybrid, what percentage of your infrastructure is on the cloud?

A: Hybrid. Approximately 50% of infrastructure is cloud-based and 50% is on-premises.

227. Q: Can we submit more than one proposal, with two different options for the solution? For example, one proposal with an AI overlay and subcontractor, and one with an in-house solution?

A: No, please submit only one proposal. Provide the solution that best aligns with the requirements of the RFP (Section 2.2, “Project Scope of Work”).

228. Q: Can we partner with more than one technology vendor?

A: Yes, but the agreement with the Harbor Department resulting from this RFP will only be with one prime consultant.

229. Q: Are you looking for a managed service, or a product with professional services?

A: We are not looking for managed services. The selected consultant shall provide professional services per the requirements in the project’s scope of work.

230. Q: How should the solution determine which incidents are "relevant" for investigation? Are there predefined criteria or thresholds?

A: The selected consultant shall provide recommendations for these criteria to the ITD project team during the design phase for review and approval.

231. Q: What is the acceptable timeframe for detecting security incidents and notifying analysts? Should it be real-time or near real-time?

A: Please refer to Question 230.

232. Q: Regarding the goal of "Provide an ease-of-use platform with a graphical user interface without extensive training for analysts" [Section 2.1], what is considered extensive for training analysts?

A: We anticipate extensive training will be required if security analysts cannot easily navigate the solution to obtain information, analysts will require frequent support from the consultant and the solution has potential hidden features that are unavailable on the GUI but instead are only available in the command line interface.

233. Q: Are there preferred LLMs or LLM providers?

A: Please refer to Question 38.

234. Q: Are there considerations for hybrid-architectures? Cloud and on-prem?

A: Please refer to Question 168.

235. Q: For the Affidavit of Company Status, we must select at least on box for Small/Very Small Business Enterprise Program, what if the contractor is not applicable to any of the selections? (SBE/VSB[E]/MBE/WBE/DVBE/OBE)?

A: It is strongly recommended that you refer to the “Tips for a Successful Proposal Submission” supplemental document that was posted on the RAMP with the RFP. If the prime is not an SBE, VSBE, MBE, WBE or DVBE, **by definition they are an Other Business Enterprise (OBE).**

236. Q: For the three client references, can we combine/use the contractor’s references and also the solution manufacturer references?

A: Yes, the proposer may combine their references and the solution manufacturer’s references.