QUESTIONS & RESPONSES #03

CONTRACT NUMBER: PA000000378
RFP/RFQ TITLE: Cybersecurity Services
CONTACT: Michelle Walker, Procurement Analyst
EMAIL: procurement@portoftacoma.com
PHONE NUMBER: 253-888-4744
QUESTIONS DUE DATE: Tuesday, October 21 @ 2:00 PM (PST)
Q&A ISSUE DATE: Monday, October 20, 2025

#	Question	Answer	Question #	Responsible for Answer	Date Received
1	Existing Users and Assets Can you confirm the total number of users (end users) supported across the 400 workstations/laptops and 180 mobile devices?	This information will be provided to the Awarded Vendor	Q-003372	Mathew	10/09/25
2	Existing Users and Assets Could you provide a detailed inventory or list of all IT assets (e.g., servers, endpoints, network devices, cloud assets, applications etc.) in scope for the cybersecurity services?	This information will be provided to the Awarded Vendor	Q-003372	Mathew	10/09/25
3	Existing Technologies Could you share a list of the current cybersecurity tools and technologies in use (e.g., SIEM, SOAR, EDR, firewalls, vulnerability scanners)?	This information will be provided to the Awarded Vendor	Q-003372	Mathew	10/09/25
4	Existing Technologies What are the primary SaaS applications (70 listed) currently in use, and are any of them considered critical or high-risk?	This information will be provided to the Awarded Vendor	Q-003372	Mathew	10/09/25
5	Requested Tools / Technologies For the Breach and Attack Simulation (BAS) requirement, is the Port expecting the vendor to provide a BAS platform license or only managed services?	Expectation is both	Q-003372	Mathew	10/09/25
6	Requested Tools / Technologies Are there any preferred vendors or platforms for SIEM and SOAR integration with the BAS solution?	Microsoft Solutions, No preference for BAS	Q-003372	Mathew	10/09/25
7	Monitoring vs. Incident Handling While the RFP mentions existing Managed Detection and Response (MDR) services with Virtual SOC, is the vendor expected to provide any additional monitoring or incident detection capabilities?	Outside of what is stated in the Milestones there is no further expectations	Q-003372	Mathew	10/09/25
8	Monitoring vs. Incident Handling Are the Red Team, Purple Team, and TTX exercises intended to supplement the existing MDR services, or are they expected to replace or evaluate them?	Evaluation Only	Q-003372	Mathew	10/09/25
9	24x7 or Other Monitoring Support Is there any expectation for 24x7 monitoring, alert triage, or incident response support as part of this engagement?	Outside of what is stated in the Milestones there is no further expectations	Q-003372	Mathew	10/09/25
10	24x7 or Other Monitoring Support If not 24x7, what are the expected hours of support or availability during the engagement period?	Dependent of Scope of the Exercise and related risk	Q-003372	Mathew	10/09/25
11	Tool Licensing Is the Port seeking only services, or is the vendor expected to provide tool licensing (e.g., for BAS platforms or password auditing tools) as part of the proposal?	Expectation is both	Q-003372	Mathew	10/09/25
12	Support Post Installation Is there any expectation for post-engagement support or ongoing assistance after the completion of each milestone?	Outside of what is stated in the Milestones there is no further expectations	Q-003372	Mathew	10/09/25
13	Support Post Installation If support is required post-installation or post-engagement, what level of support is expected (e.g., break/fix, advisory, retesting, tuning)?	Outside of what is stated in the Milestones there is no further expectations	Q-003372	Mathew	10/09/25
14	Microsoft Licensing What type of Microsoft licenses are currently in use at the Port (e.g., Microsoft 365 G3, G5, G5 Security, A3, A5)?	This information will be provided to the Awarded Vendor	Q-003372	Mathew	10/09/25
15	Microsoft Licensing Are there any plans to upgrade or change Microsoft licensing tiers in the foreseeable future?	There are no foreseeable changes to Microsoft Licensing	Q-003372	Mathew	10/09/25
16	Are References mandatory or not ?	No, references are not mandatory, but required to awarded contract.	Q-003406	Mathew	10/15/25
17	Is there a minimum number of vendors that have to bid for this RFP or PORT can select a vendor if there is only a single or < 10 bids?	No minimum number of bids is required. The Port reserves the right to select a vendor regardless of the number of bids received.	Q-003406	Mathew	10/15/25
18	If there is not enough interest can the 120k per year limit be relaxed ?	No, the annual budget cap of $120,000 (plus applicable WSST) is firm and non-negotiable.	Q-003406	Mathew	10/15/25
19	Will there be a manager or team for Knowledge transfer from previous audits, security testing and general best practices that have worked for password strength assessment ? Or the vendor team has to come up with all the new guidelines ?	Both. A designated manager and team will support knowledge transfer, including lessons learned and existing policies. Vendors are expected to build upon this foundation and propose enhancements.	Q-003406	Mathew	10/15/25
20	Invoice can be sent after a milestone and the Port of Tacoma will pay it after Milestone? How long will an average milestone usually last ?	Invoicing is not milestone-based. It is tied to the scope of work and completion of each defined exercise. The duration of each exercise will vary depending on its scope and associated risk.	Q-003406	Mathew	10/15/25
21	Can you please provide more insights about how a milestone completion is determined?	Work is not structured around milestones. Completion is determined by fulfillment of the scope of work for each exercise, assessed against deliverables and risk considerations.	Q-003406	Mathew	10/15/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
22	If vendor payments exceed milestone invoices, should vendors keep reserves, or is this unlikely?	This scenario is unlikely. The Port's scope-based payment structure is designed to align with deliverables and budget.	Q-003406	Mathew	10/15/25
23	Minimum experience of the company required?	While not explicitly stated, vendors should demonstrate relevant experience in cybersecurity services, preferably in public sector or critical infrastructure environments.	Q-003406	Mathew	10/15/25
24	Is there any mandatory certificate?	The RFP does not specify mandatory certifications	Q-003406	Mathew	10/15/25
25	Is there any mandatory minimum no. of personnel required for the services?	No minimum staffing level is mandated, but vendors must demonstrate sufficient capacity to meet the scope and timelines.	Q-003406	Mathew	10/15/25
26	Is there a current contractor providing these services? If so, could you please share their profile name with their prices?	This information is not publicly disclosed in the RFP. Vendors may submit a public records request to the Port for historical contract data.	Q-003406	Mathew	10/15/25
27	What are the current or previous bill rates associated with this contract?	The RFP reflects current cost expectations and scope. Historical rates are not specified but may be available via public records.	Q-003406	Mathew	10/15/25
28	Are there any subcontractors being used for the current contract?	If not defined within the RFP, assume no subcontractors are currently engaged.	Q-003406	Mathew	10/15/25
29	What is the estimated total number of annual hours for this contract?	This will vary based on the scope and risk profile of each exercise.	Q-003406	Mathew	10/15/25
30	Will the Port of Tacoma provide any tools, platforms, or licenses required to perform the cybersecurity exercises (e.g., BAS, password strength assessment, penetration testing), or is the vendor expected to bring and manage all necessary tooling?	See answer to question 24 above.	Q-003407	Mathew	10/16/25
31	Can the Port clarify the expected depth and scope of Red Team, Purple Team, and Breach & Attack Simulation (BAS) engagements? Are these full-scope threat emulations or limited scenario-based validations?	See answer to questions 8 above.	Q-003407	Mathew	10/16/25
32	Are there existing SIEM/SOAR platforms in use at the Port that the BAS platform must integrate with? If yes, can the Port specify the technologies or vendors involved?	See answer to questions 6 above.	Q-003407	Mathew	10/16/25
33	Should penetration testing and adversary emulation cover both Azure IaaS and SaaS applications? Are there any restrictions or exclusions for cloud-hosted services?	Yes, testing should include both Azure IaaS and SaaS applications. Any exclusions or restrictions will be defined in the scope of each exercise. Vendors should propose coverage based on risk and relevance.	Q-003407	Mathew	10/16/25
34	Are there specific threat scenarios or compliance frameworks (e.g., CISA, NIST IR 800-61) the Port prefers to simulate during TTX sessions?	Yes, the Port prefers simulations aligned with recognized frameworks such as CISA and NIST IR 800-61. Vendors may propose additional scenarios based on emerging threats and sector-specific risks.	Q-003407	Mathew	10/16/25
35	Can the Port share its data classification policy or indicate which systems/data are considered critical or regulated (e.g., PII, PCI, CJIS)?	The Port maintains a data classification policy that identifies regulated and critical systems including PII, PCI, and CJIS. Details will be shared with the selected vendor during onboarding or upon request during proposal development.	Q-003407	Mathew	10/16/25
36	Can the Port confirm whether TWIC compliance is required for all onsite engagements or only for those conducted within maritime secure terminals?	Yes, onsite engagements require TWIC compliance (but that includes having an escort if not TWIC certified). Located on Attachment B Terms & Conditions #27 (Page 21 of RFP). https://www.tsa.gov/twic	Q-003407	Michelle	10/16/25
37	Is the Vendor Cybersecurity Self-Assessment mandatory for all bidders, or only for shortlisted vendors?	Yes, per RFP page 8 "VENDOR CYBERSECURITY SELF-ASSESSMENT (Attachment E) information **MUST** be provided in an individual PDF document as a separately labeled attachment."	Q-003407	Mathew	10/16/25
38	Are certifications such as CISSP, OSCP, GPEN, CRTP mandatory for key personnel, or will equivalent experience be considered acceptable?	See answer to question 24 above.	Q-003407	Mathew	10/16/25
39	Does the Port require the auditor to be formally authorized or certified by NIST or any third-party accreditation body to conduct the NIST CSF audit?	No formal NIST or third-party accreditation is required. However, vendors must demonstrate expertise and experience in conducting NIST CSF audits, including familiarity with its domains and implementation tiers.	Q-003407	Mathew	10/16/25