QUESTIONS & RESPONSES #04
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: Tuesday, October 21, 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
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

#	Question	Answer	Question #	Responsible for Answer	Date Received
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
40	Should the Vendor hold any mandatory Certification / License at the time of submitting the Response? Please clarify.	See answer to question 24 above.	Q-003416	Mathew	10/18/25
41	On-site work might be required at the Port's facilities - security clearance and maritime access permissions will be mandatory.	Not mandatory but coordination may be required for escort	Q-003415	Mathew	10/18/25
42	Proposal must demonstrate a track record with government or critical infrastructure clients. - REFERENCES / PAST PERFORMANCE.	Cannot address any statements only questions	Q-003415	Mathew	10/18/25
43	Proven experience in government cybersecurity engagements, preferably port or transportation authorities - Strong references and prior performance documentation.	Cannot address any statements only questions	Q-003415	Mathew	10/18/25
44	Must be licensed to do business in Washington State.	Cannot address any statements only questions	Q-003415	Mathew	10/18/25
45	Must hold or be able to obtain adequate insurance coverage as specified in the RFP.	Cannot address any statements only questions	Q-003415	Mathew	10/18/25
46	Whether the Vendor can participate if we do not have ISO 27001 or SOC 2 Type II advantageous?	Yes a vendor can participate, ISO and SOC 2 are not a requirement	Q-003415	Mathew	10/18/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
47	Penetration Testing (External, Internal, Cloud, and Applications) External Testing: Approximately how many external IPs or network segments are in scope? Are any third-party hosted applications or services (e.g., hosted websites, SaaS apps) included external testing? Is there an existing vulnerability management platform in place (e.g., Tenable, Qualys)? If so, will access be provided? Will credentialed access be granted for public facing services if required? Internal Testing: Approximately how many internal IPs or network segments are in scope? How will internal access be provided? (e.g., VPN, virtual machine, physical access) Are any systems off-limits for testing (e.g., SCADA, legacy systems)? Is the internal network primarily Windows, Linux, or a mix of both? Will domain credentials be provided for auditing Active Directory? How many Active Directory domains or forests exist, and are they all in scope? Is the environment dependent on cloud/third party systems/services such as Azure, AWS, etc.? If so will these be included in scope? Will scanning agents be permitted for internal assets? Will internal testing include wireless testing? If so, approximately how many SSIDs will be included? Cloud: Which cloud platforms are in use (e.g., AWS, Azure, GCP)? What types of resources are to be tested (e.g., IaaS, PaaS, SaaS, management plane)? Will access to the cloud environment be provided for configuration review? Applications: How many applications are in scope, and what are their technology stacks (e.g., web, mobile, APIs)? Are applications developed in house or are the 3rd party provided? Will test accounts or credentials be provided? Are APIs, third-party integrations, or SSO mechanisms included in scope? Are source code reviews expected?	This information will be provided to the Awarded Vendor	Q-003409	Mathew	10/16/25
48	Red Team Adversary Emulation What are the primary objectives (e.g., data exfiltration, domain compromise, persistence, lateral movement)? What level of awareness should defenders have (covert vs. collaborative)? Are specific threat actor profiles or TTPs desired for emulation? What is the expected duration of the exercise? What detection or response capabilities are currently in place (e.g., SOC, SIEM, EDR, MDR)? Are there restrictions on social engineering, phishing, or physical intrusion?	This information will be provided to the Awarded Vendor	Q-003409	Mathew	10/16/25
49	Purple Team Exercise Who will participate from the defensive team (e.g., SOC, IR, detection engineering)? What tools or telemetry sources will be used to monitor detections (e.g., SIEM, EDR, cloud logs)? Are there specific ATT&CK techniques or kill chain phases to focus on? Will the purple team engagement build upon findings from the red team exercise? What format is preferred for collaborative sessions (in-person, remote, hybrid)? Should the engagement include training or knowledge transfer components?	This information will be provided to the Awarded Vendor	Q-003409	Mathew	10/16/25
50	Annual Password Strength Assessment Approximately how many accounts will be targeted for testing? What authentication systems are in scope (e.g., Active Directory, Azure AD, Okta, LDAP, local accounts)? Will hashed or encrypted password data be provided, or will password spraying/brute force testing be performed live? Are there policies or thresholds governing lockouts and account protections? Should the assessment include password policy review and configuration analysis?	This information will be provided to the Awarded Vendor	Q-003409	Mathew	10/16/25
51	Could you please provide detailed information about your infrastructure, including the number of routers, switches, access points, firewalls, servers, etc.?	This information will be provided to the Awarded Vendor	Q-003412	Mathew	10/17/25
52	Do you have a specified budget for this RFP? If so, could you please let us know?	The RFP does not specify a fixed budget; vendors are expected to submit a detailed cost breakdown using the provided template.	Q-003412	Mathew	10/17/25
53	Do you have an incumbent? If yes, could you please let us know their name?	This information is not publicly disclosed in the RFP. Vendors may submit a public records request to the Port for historical contract data. This information will be provided to the Awarded Vendor	Q-003412	Mathew	10/17/25
54	How many employees do you currently have?	This information is not publicly disclosed in the RFP. Vendors may submit a public records request to the Port for historical contract data.	Q-003412	Mathew	10/17/25
55	Do you require onsite support or open for Hybrid model?	Optimally any TTX Exercise will be onsite but not a requirement	Q-003412	Mathew	10/17/25
56	Could you please clarify how often you would require assessments and tests to be conducted each year?	Two TTX IR and DR, NIST Security Audit and One form of Testing e.g. Pen, Red-Purple or BSA, Password Assessment	Q-003412	Mathew	10/17/25
57	Could you please clarify whether you need the price on an annual basis or a monthly basis?	Annual	Q-003412	Mathew	10/17/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
58	NIST Cybersecurity Assessment - When was the Port's most recent NIST CSF assessment conducted? - What were the top findings or recommendations? - Have those findings been actioned or addressed?	This information will be provided to the Awarded Vendor	Q-003411	Mathew	10/17/25
59	Penetration Testing - When was the most recent penetration test performed? - What were the top findings or vulnerabilities identified? - Have those issues been remediated?	This information will be provided to the Awarded Vendor	Q-003411	Mathew	10/17/25
60	Technology and Threat Context - What SIEM solution is currently in use? - Are there specific adversary types you are most concerned about (ie insider threats, state-sponsored actors)? - Are there specific systems or functions you want to prioritize for red team, purple team, or BAS exercises?	This information will be provided to the Awarded Vendor	Q-003411	Mathew	10/17/25
61	Integration Expectations - How closely is the selected vendor expected to collaborate with the existing MDR provider and Virtual SOC service?	This information will be provided to the Awarded Vendor	Q-003411	Mathew	10/17/25
62	Testing Environment Constraints - Will testing activities (penetration, red team, purple team) be conducted in production environments, or are there dedicated sandbox/test environments?	This will be defined within the scope of each engagement-test	Q-003411	Mathew	10/17/25
63	Reporting and Presentation Format - Can the Port provide examples or templates for the expected deliverables (ie executive summary PowerPoint, technical reports) for each milestone?	This information will be provided to the Awarded Vendor	Q-003411	Mathew	10/17/25
64	Scheduling and Coordination - Are there blackout periods or specific timeframes to avoid when scheduling penetration testing or tabletop exercises?	This will be defined within the scope of each engagement-test	Q-003411	Mathew	10/17/25
65	Evaluation Criteria Clarification - In Section E.2.a, how are "innovative ideas and suggestions for enhancing the scope" weighted relative to strict adherence to the outlined milestones?	Innovative ideas and suggestions for enhancing the scope" are part of the Project Approach Narrative, which is weighted at 50 points, while adherence to milestones is embedded in the Scope of Services and evaluated through execution, not scored separately	Q-003411	Mathew	10/17/25
66	NWSA Collaboration - Since the Northwest Seaport Alliance (NWSA) is mentioned as a stakeholder in tabletop and testing exercises, what level of coordination or reporting is expected across agencies?	Single reporting, no additional coordination required	Q-003411	Mathew	10/17/25
67	Contract Terms and Clarifications - The RFP states that all contract terms are mandatory unless modified during Q&A. Can the Port confirm whether clarifying (non-material) language can be proposed during this stage?	Per RFP page 3, proposed changes to Terms & Conditions (Attachment B) need to be requested during question and answer phase of procurement. They will NOT be negociated after contract award.	Q-003411	Michelle	10/17/25
68	We would like to confirm that our understanding is correct: The Port of Tacoma is expecting a NIST Security Audit, Penetration Testing, Red Team Adversary Emulate, Purple Team Exercise, Breach and Attack Simulation (BAS), Password Strength Assessment, and a Tabletop Exercise for a firm fixed price not to exceed $120,000 annually.	Yes, all listed services are expected. However, per the RFP, the Port of Tacoma will select **one** among Penetration Testing, Red Team Adversary Emulation, Purple Team Exercise, or Breach and Attack Simulation (BAS), **in addition to** the NIST Security Audit.	Q-003418	Mathew	10/20/25
69	We would like to confirm the expected timeline for each item in scope. Is the Port of Tacoma looking to conduct and complete all listed scope of services within one fiscal year? Or are we looking to spread the scope of services out over multiple fiscal years?	Based on the RFP and as stated in question 79, the Port of Tacoma expects all listed scope of services to be conducted and completed within **one fiscal year**.	Q-003418	Mathew	10/20/25
70	We would like to confirm that no scope of service will be repeated in the potential four year contract timeframe. Assuming that no service is to be repeated, could the Port of Tacoma share the priority and order in which the scope of services will be conducted and completed by fiscal year?	The Port of Tacoma will determine the priority and order of services to be conducted and completed by fiscal year.	Q-003418	Mathew	10/20/25
71	We would like to confirm the expected timeline for Red Team Adversary Emulation and Purple Team Exercises. Are we expecting a few hours? Several days? Several Weeks? Several Months?	It depends upon scope, complexity and risk	Q-003418	Mathew	10/20/25
72	We would like to confirm this is an all-new opportunity, and that this is not a continuation of a previous opportuunity.	This scope of the RFP is not a continuation of a previous engagement.	Q-003418	Mathew	10/20/25
73	We would like to confirm if there is an incumbent. If there is an incumbent, did they perform to the satisfaction of the Port's ISO and CIO? Are they eligible to participate in this opportunity?	See question 82. There are no restrictions—any qualified vendor may submit a proposal.	Q-003418	Mathew	10/20/25
74	Does the Port of Tacoma envision team members performing various assessments such as the physical security aspects of NIST CSF 2.0 will require a valid TWIC card to examine control mechanisms? Or will the Port of Tacoma be escorting all consultants?	TWIC is not a requirement, escort can be provided if applicable to the needs of the Audit	Q-003418	Mathew	10/20/25