QUESTIONS & RESPONSES #05
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, 2025
Q&A ISSUE DATE: Friday, October 24, 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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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)?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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	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	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	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,	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)?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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	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	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	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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.?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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

#	Question	Answer	Question #	Responsible for Answer	Date Received
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
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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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	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?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	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	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	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
75	Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available?	This information is not publicly disclosed in the RFP. Vendors may submit a public records request to the Port for historical contract data.	Q-003423	Mathew	10/21/25
76	Is there a not-to-exceed budget for this project that you can share?	"The annual budget is capped at $120,000 plus applicable WA State Sales Tax."	Q-003423	Mathew	10/21/25
77	With a page limit of 18, it would be very difficult to include technical methodologies. We assume these can then be included as an appendix along with any other information that might help? The same question for items such as resumes.	"Proposals are limited to 18 numbered pages (8½ by 11 inch) excluding the cover letter, compensation information and all appendices." "Resumes of the key individuals may be included as an appendix and are not included in the total page count."	Q-003423	Mathew	10/21/25
78	Could you provide a high-level description of your overall technical operations and sensitive information/data flow so that we are able to assess the size and complexity of the engagement.	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003423	Mathew	10/21/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
79	Are you looking for (separately) Red Team and Purple Team exercises? And hence, separate quotes for each?	Yes. The RFP requests distinct Red Team adversary emulation and Purple Team exercises, each with separate deliverables and evidence requirements. Separate quotes are expected.	Q-003423	Mathew	10/21/25
80	For the Password Strength Assessment, do you intend to provide us with hashes or hash files in addition to any that we gather during penetration testing?	Yes. Hash data will be provided with explicit authorization. Testing will be offline, with no live login attempts. All recovered credentials must be securely handled and destroyed post-reporting.	Q-003423	Mathew	10/21/25
81	For external network penetration testing/vulnerability assessment, please provide the approximate number of live external IPs in scope.	Specific IP counts will be provided to the awarded vendor. General perimeter architecture may be available via public records request.	Q-003423	Mathew	10/21/25
82	For internal network penetration testing/vulnerability assessment, please provide the approximate number of live internal IPs in scope.	Internal IP scope details will be shared with the selected vendor under NDA.	Q-003423	Mathew	10/21/25
83	For web application penetration testing, please provide the number of web applications in scope. Also, confirm if you will be providing test accounts.	The Port utilizes a range of SaaS and internal applications. Final scope and test account provisioning will be coordinated with the awarded vendor.	Q-003423	Mathew	10/21/25
84	If wireless network penetration testing is in scope, please provide the total number of locations to be tested. Also, is sampling permitted or are all locations to be tested?	Wireless testing scope will be finalized with the selected vendor. Sampling may be permitted based on risk profile and operational coverage.	Q-003423	Mathew	10/21/25
85	For social engineering penetration testing, please provide the number and types of scenarios you would like us to perform. Also, provide the number of end users/employees to be targeted.	Scenarios may include phishing, vishing, and physical access. Target groups and counts will be defined collaboratively with the awarded vendor.	Q-003423	Mathew	10/21/25
86	Is there any other type of penetration testing (e.g. mobile apps, etc.) required? If so, please provide details sufficient for us to be able to scope the engagement.	Mobile apps and APIs may be in scope. Specific platforms and access requirements will be shared with the selected vendor.	Q-003423	Mathew	10/21/25
87	NIST Security Audit: Scope – Should the CSF audit cover the entire enterprise (on-prem, cloud, SaaS) or only specific systems/business units? Framework Use – Do you want results strictly against NIST CSF v2.0, or also mapped to other standards (e.g., NIST 800-53, 800-171, ISO 27001)? 800-53 Alignment – If mapping to NIST 800-53 is expected, should alignment be to Rev. 5 (current) or Rev. 4 for legacy consistency? Policies – How many distinct system- or business-unit-specific policies should we expect to review, or are most controls governed by centralized enterprise policies? Deliverables – Beyond the required control spreadsheet and executive summary, do you want detailed remediation guidance or just risk ratings?	The audit should cover the entire enterprise, including on-prem, cloud, and SaaS environments.	Q-003425	Mathew	10/21/25
88	Incident Response and Disaster Response Tabletop Exercise (TTX): Objectives – What are the primary goals of the exercise (e.g., test incident response plan, validate communications, evaluate leadership decision-making, cross-team coordination)? Scenario Preference – Do you want the scenario to focus on a cyber event only (e.g., ransomware, cloud breach, insider threat) or a combined cyber/operational impact event (e.g., disruption to port operations or supply chain)? Participant Roles – Which groups will participate (IT/security, operations, communications, legal, leadership), and do you want scenarios tailored to executive decision-making vs. technical response? Frameworks – Do you want the exercise structured against a recognized framework (e.g., NIST SP 800-84, FEMA HSEEP, CISA TTX templates) or more of a custom scenario-driven workshop? Existing Plans/Playbooks – Should the exercise be structured to validate your current IR/DR plans as written, or to stress-test gaps where procedures aren't fully documented? Complexity Level – Do you want a single scenario walkthrough, or a more complex exercise with multiple injects and branching decisions?	Prefer NIST CSF v2.0 with optional mapping to NIST 800-53 Rev. 5 and ISO 27001 for broader alignment.	Q-003425	Mathew	10/21/25
89	Could the PORT please confirm whether this is a new initiative or an existing engagement?	Use Rev. 5 for current alignment; Rev. 4 may be referenced for legacy systems.	Q-003424	Mathew	10/21/25
90	Could the PORT provide an estimated budget or a Not-to-Exceed (NTE) amount for this contract?	Most controls are governed by centralized policies. Specific unit policies will be identified if applicable.	Q-003424	Mathew	10/21/25
91	Could the PORT please provide the anticipated project timeline, including key milestones and the overall expected duration of the	Include control spreadsheet, executive summary, and detailed remediation guidance.	Q-003424	Mathew	10/21/25
92	Could the PORT please clarify whether it intends to award this RFP to a single vendor or multiple vendors? If multiple awards are anticipated, could the PORT specify the expected number of vendors to be selected?	All CSF audit activities may be conducted remotely. Tabletop exercises will be in person.	Q-003424	Mathew	10/21/25
93	Can you please confirm the expected frequency of each service (e.g., will all three activities—NIST Audit, Security Testing, and	Validate IR/DR plans, leadership decision-making, and cross-team coordination.	Q-003424	Mathew	10/21/25
94	For budgeting purposes, should pricing assume all services every year, or that the Port will select specific ones each year within the annual $120,000 limit?	Prefer combined cyber/operational impact scenarios (e.g., ransomware affecting port logistics).	Q-003424	Mathew	10/21/25
95	Are vendors allowed to propose optional add-ons or pricing tiers (e.g., different levels of testing or reporting detail)?	Include IT/security, ops, legal, comms, and executive leadership. Scenarios will be tailored to both strategic and technical roles.	Q-003424	Mathew	10/21/25
96	Will the Port provide remote access or require onsite presence for any activities? If onsite work is expected, how many visits per year should be included? Should travel and lodging be priced as separate reimbursable expenses or included in fully burdened rates?	Use NIST SP 800-84 or CISA templates for structure.	Q-003424	Mathew	10/21/25
97	Is the Port expecting firm fixed pricing per milestone or a time-and-materials model with not-to-exceed limits?	Exercise will validate current plans and expose undocumented gaps.	Q-003424	Mathew	10/21/25
98	Are subcontractors allowed for specialized testing areas (e.g., Red Teaming or BAS platform licensing)?	Prefer multi-inject scenarios with branching decisions.	Q-003424	Mathew	10/21/25
99	Will the same vendor be expected to perform all activities (audit, testing, exercises), or may separate vendors be considered for	Map findings to NIST CSF Respond/Recover and 800-53 controls.	Q-003424	Mathew	10/21/25
100	**NIST Cybersecurity Framework Audit (v2.0)** Which systems and departments will be in scope for the NIST CSF audit?	Planning meetings can be remote. Stakeholder interviews may be scheduled.	Q-003424	Mathew	10/21/25
101	**NIST Cybersecurity Framework Audit (v2.0)** Will interviews and workshops with staff be conducted onsite or virtually, and approximately how many stakeholders are expected to	Please confirm if this is a new initiative or continuation.	Q-003424	Mathew	10/21/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
102	**NIST Cybersecurity Framework Audit (v2.0)** Could the Port please clarify the approximate number of employees and IT users that fall within the scope of the NIST CSF audit?	The annual budget is capped at $120,000 plus applicable WA State Sales Tax.	Q-003424	Mathew	10/21/25
103	**Security Testing & Validation** **Penetration Testing** How many external IP addresses, internal segments, and applications will be in scope?	The contract begins January 12, 2026, with two optional one-year renewals for a total of up to four years.	Q-003424	Mathew	10/21/25
104	**Security Testing & Validation** **Penetration Testing** For web and cloud testing, are applications hosted on Azure, SaaS, or custom-built environments?	The PORT anticipates awarding one (1) contract.	Q-003424	Mathew	10/21/25
105	**Security Testing & Validation** **Penetration Testing** Should the proposal include social engineering (phishing/vishing) or is testing limited strictly to network and application layers?. If yes please tell the frequency like monthly/ weekly and how many users?	All three activities are scoped for annual execution at the discretion of the PORT.	Q-003424	Mathew	10/21/25
106	**Security Testing & Validation** **Red Team Adversary Emulation** What scope or scenario types should the Red Team focus on (e.g., data exfiltration, privilege escalation, phishing)?	Pricing should assume all services annually unless otherwise directed by the PORT.	Q-003424	Mathew	10/21/25
107	**Security Testing & Validation** **Red Team Adversary Emulation** How many targets or departments will be included in the emulation exercise?	Yes, vendors may propose optional add-ons and tiered pricing.	Q-003424	Mathew	10/21/25
108	**Security Testing & Validation** **Red Team Adversary Emulation** Is there a preferred duration (e.g., 2 weeks, 4 weeks) for the engagement?	Dependent on the scope of work in respect to the exercise	Q-003424	Mathew	10/21/25
109	**Security Testing & Validation** **Purple Team Exercise** How many sessions or workshops does the Port expect each year?	NIST, Exercise and Two TTX	Q-003424	Mathew	10/21/25
110	**Security Testing & Validation** **Purple Team Exercise** Will Purple Team exercises use the Port's existing SIEM and SOAR environment for live detection tuning?	Yes	Q-003424	Mathew	10/21/25
111	**Security Testing & Validation** **Purple Team Exercise** Does the Port prefer a tool-assisted approach (using attacker emulation platforms) or manual collaborative testing?	Both and dependent upon the scope of the exercise	Q-003424	Mathew	10/21/25
112	**Security Testing & Validation** **Breach & Attack Simulation (BAS)** Does the Port currently have a BAS platform (e.g., AttackIQ, Cymulate), or should the vendor provide and manage one?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003424	Mathew	10/21/25
113	**Security Testing & Validation** **Breach & Attack Simulation (BAS)** Should the pricing include annual licensing for the BAS software?	Vendor will provide solution if this exercise is Scoped and deemed of value to the Port/NWSA	Q-003424	Mathew	10/21/25
114	**Security Testing & Validation** **Breach & Attack Simulation (BAS)** What level of integration with SIEM/SOAR tools is expected (API-level or manual report sharing)?	Dependent upon the scope of the specific exercise and will be defined at that time	Q-003424	Mathew	10/21/25
115	**Security Testing & Validation** **Breach & Attack Simulation (BAS)** How often does the Port expect continuous validation runs (monthly, quarterly, etc.)?	Dependent upon the scope of work for each exercise and findings	Q-003424	Mathew	10/21/25
116	**Security Testing & Validation** **Annual Password Strength Assessment** Approximately how many user accounts will be included (Active Directory + cloud)?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003424	Mathew	10/21/25
117	**Security Testing & Validation** **Annual Password Strength Assessment** Will the Port provide hashes directly, or is vendor extraction assistance required?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003424	Mathew	10/21/25
118	**Security Testing & Validation** **Annual Password Strength Assessment** Are there specific hash types or systems in use (NTLMv2, bcrypt, AzureAD)?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003424	Mathew	10/21/25
119	**Security Testing & Validation** **Annual Password Strength Assessment** Should the pricing include two rounds (initial test + post-remediation verification)?	This will be dependent upon the scope of the exercise and findings and risk will determin the need for post remediation recommendations	Q-003424	Mathew	10/21/25
120	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** How many TTX sessions are expected per year (one or multiple)?	Ideally two, IR and DR	Q-003424	Mathew	10/21/25
121	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** Will these be joint exercises with the Northwest Seaport Alliance, or strictly Port of Tacoma staff?	Port of Tacoma and Northwest SeaPort Alliance for purpose of this RFP is one entity	Q-003424	Mathew	10/21/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
122	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** Will the vendor be responsible for developing all scripts and materials, or will the Port provide initial scenarios?	Each exercise for scope and scenarios wil be developed jointly	Q-003424	Mathew	10/21/25
123	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** What types of incidents should scenarios focus on (ransomware, insider threat, supply chain, etc.)?	Each exercise will have its own scope developed to determine this based on the need, threat landscape and risk	Q-003424	Mathew	10/21/25
124	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** Are in-person facilitators required, or is a virtual option acceptable?	Virtual option is acceptable	Q-003424	Mathew	10/21/25
125	**Security Testing & Validation** **Incident Response / Disaster Recovery Tabletop Exercises (TTX)** How many participants are typically expected per session (the RFP mentions 20–30; please confirm)?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003424	Mathew	10/21/25
126	Could the Port confirm whether the $120,000 annual ceiling is a firm cap for all activities combined, or whether there is flexibility to phase or rotate certain testing and audit activities over the potential four-year contract term (e.g., NIST audit in Year 1, Red Team in	Flexibility to phase a certain number of exercises annually exists	Q-003426	Mathew	10/21/25
127	Is the Port's primary objective regulatory assurance (NIST compliance validation), threat simulation and detection improvement	Combination thereof	Q-003426	Mathew	10/21/25
128	Would the Port consider a multi-year workplan that allocates specific services per year to maintain alignment with the budget	Yearly and Multi Year Planning and Scheduling are allowed	Q-003426	Mathew	10/21/25
129	For the NIST CSF 2.0 audit, is the intent a full control-by-control maturity assessment across all 108 subcategories, or a targeted	A scope will be agreed upon prior to the exercise in which this would be determined	Q-003426	Mathew	10/21/25
130	Can all assessment activities, including committee briefings, be delivered remotely?	Yes	Q-003426	Mathew	10/21/25
131	Regarding penetration testing, could the Port specify the approximate number of internal hosts, external IPs, and web/cloud ap	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003426	Mathew	10/21/25
132	For the Red Team exercise, will the Port require a multi-phase adversary emulation (reconnaissance, lateral movement, privilege	Dependent upon scope of work	Q-003426	Mathew	10/21/25
133	Will social engineering or phishing simulation be within scope of the Red Team activity?	If defined within scope	Q-003426	Mathew	10/21/25
134	Can red team exercises and reporting be conducted remotely?	Yes	Q-003426	Mathew	10/21/25
135	Are there specific threat actor profiles or tactics the Port wants emulated?	This information will be provided to the awarded vendor	Q-003426	Mathew	10/21/25
136	For the Purple Team, is the objective to deliver a real-time detection-tuning exercise with the Port's MDR/SOC provider, or a tabletop-	Real Time	Q-003426	Mathew	10/21/25
137	Regarding Breach and Attack Simulation (BAS), should the bidder assume responsibility for providing and operating the BAS platform, or leveraging an existing solution used by the Port or its MDR provider?	Vendor to provide their own platform	Q-003426	Mathew	10/21/25
138	What SIEM/SOAR platforms are in use for integration?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003426	Mathew	10/21/25
139	Can BAS setup, monitoring, and reporting be performed remotely?	Yes	Q-003426	Mathew	10/21/25
140	What is the expected frequency and scope of simulations?	Scope to be determined each exercise, frequency per the RFP is annual	Q-003426	Mathew	10/21/25
141	For the Annual Password Strength Assessment, how many user accounts are expected to be included, and will service or privileged accounts be excluded as per the Rules of Engagement?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003426	Mathew	10/21/25
142	Can the Port confirm which activities require in-person delivery (e.g., TTX, presentations) versus those that may be conducted	No In Person Requirement Defined in RFP	Q-003426	Mathew	10/21/25
143	Are travel and lodging expenses expected to be included within the $120,000 ceiling or reimbursed separately under Washington	Yes no additional cost should create and excess of costs beyond the budgeted amount	Q-003426	Mathew	10/21/25
144	Will the Port's existing MDR/SOC provider participate in Purple or BAS exercises, and if so, can the vendor assume access to	Yes	Q-003426	Mathew	10/21/25
145	Can milestone structures be proposed collaboratively?	Yes that is the expectation	Q-003426	Mathew	10/21/25
146	Is there flexibility in how project management and reporting time is allocated?	Yes there is flexibility just so much as the defined results are timely and agreed upon	Q-003426	Mathew	10/21/25
147	Are regular status updates expected, and if so, at what frequency?	Yes, timing to be agreed upon	Q-003426	Mathew	10/21/25
148	Does the Port expect technical and executive reports for each testing element, or a single consolidated annual report?	Yes, both artifacts need to be created and presented	Q-003426	Mathew	10/21/25
149	Will vendors be expected to present findings separately to both the Cybersecurity Oversight Committee and the IT Steering	Yes, that possibility could exist depending upon scope of the exercise	Q-003426	Mathew	10/21/25
150	Are remediation validation tests (re-tests) expected within the same annual cycle, or handled as follow-on tasks?	This is dependent upon critical or high findings	Q-003426	Mathew	10/21/25
151	What is the expected turnaround time for each report after activity completion?	Thirty Days	Q-003426	Mathew	10/21/25
152	Are executive summaries and technical appendices required for each service?	Yes	Q-003426	Mathew	10/21/25
153	Is there a centralised portal or system for submitting deliverables?	To be agreed upon by the Port and Service Provider	Q-003426	Mathew	10/21/25
154	Would the Port consider a time-and-materials (milestone-based) pricing model within the $120,000 cap, allowing scope adjustment as	This would be dependent upon the agreed scope of work for each individual exercise	Q-003426	Mathew	10/21/25
155	Is it acceptable to propose optional task orders for activities that may exceed the base budget (e.g., full Red Team or BAS	This would be defined and agreed upon in the scope of an exercise	Q-003426	Mathew	10/21/25
156	Could the Port confirm whether sales tax is to be applied on top of or included within the $120,000 ceiling?	Yes per Washington State Sales Tax regulations	Q-003426	Michelle	10/21/25
157	Will subcontractors or specialist partners (e.g., for BAS or password recovery services) be permitted under this RFP?	Can be considered within the scope of each exercise	Q-003426	Mathew	10/21/25
158	Can appendices (e.g., resumes, case studies) be excluded from the page count?	Yes	Q-003426	Michelle	10/21/25
159	Will oral presentations be conducted remotely?	Yes via Teams	Q-003426	Michelle	10/21/25
160	Is there a preferred structure or format for the proposal beyond what's stated?	Table of contents and in order of evauation criteria.	Q-003426	Michelle	10/21/25
161	**Breach & Attack Simulation (BAS)** Scope & cadence: Is BAS intended as a one-time engagement, periodic (e.g., quarterly), or continuous?	Annual if chosen as the appropriate exercise for the year and agreed upon within the scope of work provided to the port for the individual BAS exercise	Q-003427	Mathew	10/21/25
162	**Breach & Attack Simulation (BAS)** Delivery model: Do you prefer a platform-based continuous BAS or a consulting-led simulation with reporting?	Delivery model will be agreed upon between the Port and the Vendor to determine the correct path	Q-003427	Mathew	10/21/25

#	Question	Answer	Question #	Responsible for Answer	Date Received
163	**Breach & Attack Simulation (BAS)** Focus areas: Should we emphasize specific attack vectors (phishing, lateral movement, data exfiltration, privilege escalation) or run	All options are on the table and can be discussed and agreed upon within the scope of the exercise	Q-003427	Mathew	10/21/25
164	**Breach & Attack Simulation (BAS)** Environment: Run in production or a controlled/test environment? Any systems or segments to exclude?	To be defined within the scope of work and risk assesment	Q-003427	Mathew	10/21/25
165	**Breach & Attack Simulation (BAS)** Framework alignment: Should BAS map findings to MITRE ATT&CK, NIST CSF/800-53, or CIS Controls?	To be defined within the scope of work - this information will also be provided to the awarded vendor	Q-003427	Mathew	10/21/25
166	**Breach & Attack Simulation (BAS)** Deliverables: What's most useful—Executive summary, technical report, prioritized remediation plan, and/or ongoing	To be defined within the scope of the exercise in respect to deliverable and presentable artifacts	Q-003427	Mathew	10/21/25
167	**Breach & Attack Simulation (BAS)** Integrations: -What SIEM are you using (vendor/version)? -What SOAR platform (if any)? -Any ticketing/ITSM (ServiceNow/Jira) we should integrate with?	Due to the sensitivity of our cybersecurity architecture, specific details will be provided to the awarded vendor under appropriate confidentiality agreements. General operational scope may be available via public records request.	Q-003427	Mathew	10/21/25
168	Must respondents quote for all line items?	Respondents can quote at thier own discretion	Q-003429	Mathew	10/21/25
169	I wanted to ask about the payment for this RFP. I'm curious if the amount to be paid, per year, is a typo or if it truly is 120 thousand a year? Just a NIST assessment can cost upwards of 100 thousand. Each service asked for is a lot to do and is charged typically much higher. As we would love to bid on this, it's in our specialty, it just isn't possible for the amount listed. Thanks for clarifying or	"The annual budget is capped at $120,000 plus applicable WA State Sales Tax."	Q-003432	Mathew	10/21/25