QUESTIONS & RESPONSES #02

RFP / TITLE	**071855-Cybersecurity Auditor 2023**
CONTACT	**Michelle Walker, Contracts & Procurement Analyst**
EMAIL	**procurement@portoftacoma.com**
PHONE NUMBER	**253-888-4744**
SUBMITTAL DUE DATE	**3/10/2023**
Q&A ISSUE DATE	

	Question	Answer	Question #
1	Please let us know what is the number of end users in scope for this assessment.	Approximately 300 users	Q-001540
2	Are you looking for a gap assessment or a formal assessment with certification?	Gap Assessment	Q-001546
3	How many locations are in-scope?	3-5 sites	Q-001546
4	How many disaster recovery locations are in-scope?	2	Q-001546
5	How many IT personnel will be in-scope?	20	Q-001546
7	How many systems (i.e., servers, workstation) are in-scope of the assessment?	See information in the RFP	Q-001546
8	How many employee users can access systems within the scope?	See answer to question #1.	Q-001546
9	How many systems are accessible from the internet?	None	Q-001546
10	What third party vendors/managed service providers does the organization use that access internal systems or affect the security of the environment? (Ex: Managed information technology services or by vendor support maintenance contract)	Yes, the Port does have external MD&R services and a host of vendor supported contracts.	Q-001546
11	Please list any leverage cloud services used (either Infrastructure-as-a-Service or Software- as-a-Service) (Ex: Amazon Web Services)?	Azure (IaaS, SaaS), AWS 3rd-party hosted applications	Q-001546
12	Do we have to submit an intention or interest to bid for this proposal?	No, just sign up for the Holder's List so you will be notified when we add documents or change anything.	Q-001545
13	RFP 071855 (Cybersecurity Auditor 2023) references “Attachment A – Instructions for Proposing” and states that it is attached to the RFP; however it appears to be missing. In order to fully evaluate the RFP, can you please provide Attachment A ahead of the question submission date?	Addendum 01 & Updated RFP document.	Email
14	When was the last agencywide risk assessment performed?	Don't know	Q-001552
15	Did the risk assessment include IT and Cybersecurity risks?	No	Q-001552
16	Do these IT risk assessments include or consider outsourced functions, third parties, and business partners?	No	Q-001552
17	What does the Port currently consider to be its most serious cybersecurity risks?	The human elemnet	Q-001552
18	What is the current maturity of the Port’s cybersecurity framework?	According to the NIST CSF Implementation Tiers the Port is a Tier 3 – Repeatable	Q-001552
19	Has the Port formally documented data classification and prioritization of systems?	Yes	Q-001552
20	Where does principal responsibility for overseeing cybersecurity reside within the Port (i.e., CISO, CIO, Cybersecurity Risk Officer, Director of IT, etc.)?	Director of IT	Q-001552
21	Does the Port maintain established roles and responsibilities over cybersecurity?	Yes	Q-001552
22	Does the Port have a security incident response plan?	Yes	Q-001552
23	Does the Port perform Tabletop exercises periodically?	Yes	Q-001552
24	Has the Port been subject to a material cybersecurity incident or data breach in the last 12 months?	No data breach incidents in the past 12 months	Q-001552
25	What is the minimum number of references (recent contracts/projects in the last five years as completed by key members of the project team) we should include in our proposal?	3	Q-001552
26	Is the intention to conduct milestones 1 through 4 once each year during the initial three-year period?	Yes	Q-001581

27	How many staff members are serving IT support functions?	See Answer to question #5	Q-001581
28	How many staff members are serving cybersecurity support functions, and are these people already accounted for in the count of IT support?	Yes.	Q-001581
29	Does the Port of Tacoma utilize any third-party vendors for support of IT or networking infrastructure?	See Answer to question #10	Q-001581
30	Under proposal format: Does Port of Tacoma have a preferred font type?	Easily readable	Q-001581
31	Is there any mandatory percentage goal for the Office of Minority and Women's Business Enterprises (OMWBE) for this contract? If so, please disclose the percentage.	See RFP Page 9 "SMALL BUSINESS AND DISADVANTAGED BUSINESS OPPORTUNITIES"	Q-001581
32	Qualifications & Experience require us to include working titles, degrees, certificates, and licenses of the resources. By this request, do you need scanned documents of the originals?	Listing of the degrees, certificates, and licenses of the resources is sufficient. Copies of the certificates, degrees, or licenses is not required for the proposal.	Q-001581
33	Qualifications & Experience require us to include working titles, degrees, certificates, and licenses of the resources. Can we provide complete resumes where working titles, degrees, certificates, and licenses are mentioned?	Yes	Q-001581
34	Section 3. Compensation. What is the desired format? Can we present an excel spreadsheet of a chart detailing the requirements and respective costs?	Please submit in PDF format. See RFP page 7 "Procurement Submission Portal Instructions"	Q-001581
35	During the final evaluation phase, Oral presentation. Can it be web-based or does a representative of the firm will have to visit the Port of Tacoma offices?	Can be onsite or virtual	Q-001581
36	Is it required to provide the COI alongside the proposal response?	No, only required after award and signed contract.	Q-001581
37	Could the agency grant a due date extension?	No	Q-001581
38	Is there any incumbent for this project? If so, please disclose the name.	Moss Adams	Q-001581
39	If the resources we provide at the time of proposal submission are not available at the time of a potential contract award could we replace them with equally qualified resources?	Yes	Q-001581
40	Is it allowed to use digital signatures to sign the forms?	Yes. We will send documents for signatures using Adobe Sign.	Q-001581
41	Does the agency require wet ink signatures?	See Answer to question #40	Q-001581
42	Does the agency accept remote resources to work on the project?	Yes, as long as they are not offshore resources.	Q-001581
43	Does the agency prefer on-site resources to execute the project?	The presentation can be either why however, the virtual presentation must be on video.	Q-001581
44	Is it required to provide the attachment E with the proposal response?	The RFP does not request an Attachment E	Q-001581
45	Please confirm that Port of Tacoma only wants the NIST CSF controls spreadsheet as the deliverable for Milestone 1, not the spreadsheet plus a formal management report.	Yes a spreadsheet is required as the deliverable.	Q-001580
46	Because “auditor services” is prominently referenced, does the Port require a cybersecurity expert with auditor credentials, such as ISO Leader Auditor, or are you using the term auditor more generically?	The term auditor is not used in a general sense. Yes, the Port intends for staff to have security auditor credentials.	Q-001579
47	Does the Port accept California-certified SBEs, MBEs, and DBEs in reciprocity, or must these be Washington-certified?	The firm simply must provide proof of security auditor credentials	Q-001579
48	Is Attachment C (Cost Breakdown) only to be completed for Year 1?	Costs should be annual costs. See also Answer to question #26	Q-001579
49	Does the Port allow an inflation factor for follow-on costs for the additional contract years, as hinted in Attachment B, Section 25. D Rates?	Rate adjustments are tied to CPI as specified in Attachment B, Section 25 d. Rates.	Q-001579
50	Are costs required for the initial 3 years, or for all 5 years?	Costs specified should be annual costs for the duration of the contract.	Q-001579
51	Does the Port expect each of the (up to) 5 years’ costs to be borne at the level rate of $80,000 per year, or will you accept a varying mix of fees over the contract years that may either exceed or be less than $80,000?	Costs should not exceed $80,000 annually	Q-001579
52	Section B Scope of Services – Is the assessment to be on-site and technically validated with evidence, or virtual, trust-based, without evidentiary validation?	Either way is acceptable.	Q-001579
53	Is Milestone 4 (Executive Briefing) to be on-site and in person, or also virtual like Milestone 2?	Either way is acceptable.	Q-001579
54	What department is the buyer within the Port (e.g., internal audit, cybersecurity, risk management, IT, or other)?	IT	Q-001579
55	For each year, when do you want the audit completed?	July	Q-001579
56	Do you prefer us to perform this engagement remotely, on-site, or both? (if on-site, please indicate location(s) to visit?	See answer to question #52	Q-001579
57	Is the expectation for RFP interviews to be onsite or will it be virtual?	Either way is acceptable.	Q-001579

58	Does this audit need to incorporate the need to evaluate the operating effectiveness of the NIST CSF controls over a period of time or should we treat it as an independent audit with no control testing involved?	Since this is a new contract the Port is expecting an independent audit in year one. This would get a new set of eyes looking at the Port's cyber program. The subsequent years can report the effectiveness over time.	Q-001579
59	Will the selected firm have visibility to existing Service Level Agreements with Vendors that provide IT/Cyber/Privacy-related services?	Yes	Q-001579
60	Please describe the roles and responsibilities for the respective roles in the IT function.	There are 24 IT positions that consist of management, networking and systems infrastructure, service desk, application support teams, and project managers.	Q-001579
61	Other than the Port's ISO and IT Director, how many other individuals should we be prepared to interview on the business-side as well as vendors for processes that they may manage or oversee, and what are their respective functions? (8 major departments and functions at the Port in addition to IT, and the Virtual SOC,)?	Follow the NIST CSF to determine the necessary resources to interview.	Q-001579
62	Will the scope include scope The Northwest Seaport Alliance organization? If the organization needs to be in-scope, please provide similar information of background noted in the RFP 071855 that is applicable to The Northwest Seaport Alliance organization? (IT system overview, cybersecurity program overview, key stakeholders to interview, etc.).	Just the Port of Tacoma is in scope.	Q-001579
63	Can you describe the status of existing IT/Security-related policies, standards, procedures, plans, and guidelines and what currently exists/are enforced?	Expect all the industry-related documentation when auditing the IT department.	Q-001579
64	Requested Changes to the Port's Standard Terms and Conditions 1. Section 6B. Ownership of Intellectual Property. While the Instruments of Service naturally include deliverables, the Consultant's internal or draft documentation are the Consultant's intellectual property and should not be a substitute for the Port's own records. We request that Section 6B be struck except for the last sentence, or alternatively, that it be worded as follows: "The Instruments of Service shall not include any calculations, notes, draft documents, reports, drawings, specifications, electronic files, including e-mails, and any of the Consultant's other internal materials, information or documentation developed or prepared in the performance of the Services. The Consultant shall obtain no proprietary rights or interest the Instruments of Service." 2. Section 23(b)(i). Insertion of sentence: "Required limits may be a combination of primary CGL policy and Umbrella/Excess Liability policy(ies)." 3. Section 23(b)(v). Insertion of sentence: ""Required limits may be a combination of primary Employer's Liability policy and Umbrella/Excess Liability policy(ies)." 4. Section 23(c). Consultant's insurers' policies include additional insured under a blanket policy instead of naming by endorsement. Modify third and fourth sentences to read: "Except for Professional Liability and Workers' Compensation/Employer's Liability, the Port and the Northwest Seaport Alliance shall be included as an additional insured on all policies on ISO Form CG 20 10 Form B or equivalent. Except for Workers' Compensation and Professional Liability, waivers of subrogation shall be provided on all policies where permitted by law."	Port Currently Reviewing	Q-001579
65	How long ago was the last assessment?	If I understand the question, it was a 1-week auditing engagement that included 20+ one-hour interviews during the week. In addition, there were 3-weeks of providing requested documentation for the auditors to review.	Q-001578
66	Are you currently outsourcing this initiative or is this internally led?	Outsource	Q-001578
67	Are there any current NIST compliance software/technology vendor solutions in your environment?	Yes	Q-001578
68	On page 9 - Can you please confirm/specify where the WBE needs to be registered ie at the state/federal/ level?	See answer to question #38.	Q-001578
69	RFP has IT assets . Does the assessment need to cover only IT assets? What is the scope of the OT assets (please share relevant inventory , if any) ?	No, the Port will not share inventories at this stage of the process. However, Asset Management is part of the NIST CSF.	Q-001577
70	Will Port of Tacoma share the previous VA-PT reports to Consultant , for review as part of the NIST CSF assessment ?	No, the Port will not share previous audit documentation.	Q-001577

71	Would Port of Tacoma allow VA-PT tools /utilities would be allowed to run for testing the security as part of the assessment?	It depends.	Q-001577
72	Would it be only a process-based/ document review-based assessment ?	Both	Q-001577
73	Whether Consultant would be allowed to have discussions/reviews with IT Service Providers / Managed Security Service Providers of Port of Tacoma ?	Not in the past.	Q-001577
74	Will the scope of the assessment cover just IT systems, or also OT/SCADA systems?	Primarily the 108 controls in the NIST CSF	Q-001576
75	As a small business, we have found that it is difficult to find insurance companies willing to cover the level of insurance for the type of work requested as detailed within the RFP. We are requesting an official change to reflect the following insurance levels, which are in accordance with the risk, contract, and services we will provide: oCommercial/General Liability: Lower the requirement for Aggregate from $4,000,000 to $2,000,000 oAutomobile Liability: Lower the requirement from $2,000,000 to $1,000,000 oStop/Gap Employers Liability: Waive this requirement since it is not applicable oProtection and Indemnity Insurance/Jones Act: Waive this requirement since it is not applicable oMaritime Employers Liability: Waive this requirement since it is not applicable	o Commercial/General Liability: Lower the requirement for Aggregate from $4,000,000 to $2,000,000 – **NOT Acceptable-This as aggregate limits are shared between all claims in the policy period. If this is an issue, I am willing to revisit it. I noticed another question about an umbrella policy, that would be an acceptable method to achieve the aggregate.** o Automobile Liability: Lower the requirement from $2,000,000 to $1,000,000 – **Acceptable** o Stop/Gap Employers Liability: Waive this requirement since it is not applicable – **If the company has employees, it is applicable and accordingly, NOT acceptable** o Protection and Indemnity Insurance/Jones Act: Waive this requirement since it is not applicable - **Acceptable** o Maritime Employers Liability: Waive this requirement since it is not applicable - **Acceptable**	Q-001576
76	Do you require security testing to be performed, or just interviews/documentation review? If yes, what security testing do you want?	Interviews only	Q-001576
77	We would like to request an annual escalation of 2.5% for our quoted rates.	No	Q-001576
78	Is the Port currently aligned with the NIST CSF	Yes	Q-001575
79	The annual third-party audits that have been done for the last 3 years – were those also against the NIST CSF?	Yes	Q-001575
80	How many documented policies/procedures does the Port have? Are they aligned with the NIST CSF?	See answer to question # 63. Yes most align with the CSF.	Q-001575
81	Will the winning firm have access to the prior years' audit reports and recommendations?	No	Q-001575
82	How many IT staff does the Port have? Of these, how many are dedicated to cybersecurity?	See question #1 and 1	Q-001575
83	Please confirm whether technical testing (e.g. device configuration reviews or application testing) is in scope as a part of the IT security performance audit?	No this is not in scope.	Q-001575
84	Is there a physical onsite component of this audit?	The audit consists of interviews. Which for the most part are virtual.	Q-001575
85	The RFP asks responders to "Include a summary of innovative ideas and suggestions for enhancing the scope of services". Please elaborate on other desired service for your organization, or clarify if marketing material / service menus are desired. We value your reviewers time want to include only the most relevant information in our response.	The primary focus is the scope of work in the RFP. If there are ideas or suggestions the Port would consider them.	Q-001575
86	Is your organization undertaking any other IT or cybersecurity initiatives at this time?	Yes	Q-001575
87	Have there been any recent cybersecurity incidents in your organization?	None that had a data breach.	Q-001575
88	Is there a local preference associated with the solicitation?	The work can be completed on-site or virtually. Please specify your preferred approach in your proposal.	Q-001574
89	How many documented policies and procedures does the Port have documented?	This audit is focusing on the NIST CSF and the associated documents in the framework.	Q-001574
90	How many IT personnel does the Port employ, and is IT centralized?	23 IT staff and IT is centralized.	Q-001574
91	Is there an incumbent for this project? If so, who is the incumbent?	See anwser to question # 38.	Q-001569
92	Does the Port have an anticipated start time for the first year of the project?	The Port considers this as an audit not a project. See answer to question # 55.	Q-001569
93	Does the Port have an anticipated completion date for the first year of the project?	Since this is an audit and the Port would expect completion within 4 weeks after the completion of the interview week.	Q-001569
94	On pages 2-3 of the RFP, the Port states "The Port will select a qualified cybersecurity auditor on the best value basis using a point method of the award, to undertake a comprehensive IT Security Performance audit. This will include a thorough review of the Port's Cybersecurity Program." Please provide additional information on what the "thorough review of the Port's Cybersecurity Program" will entail. (specific assessments to be conducted, in-scope areas of the cybersecurity program to focus on, etc.)	The framework is the NIST CSF. The Port expects a week of the necessary interview with staff/SMEs. And the review of all the corresponding documentation called out in the framework.	Q-001569

95	Should the price given for Milestone 1, listed as "The results of the assessment will be documented on a spreadsheet for each of the CSF controls with risk finding rated as high, medium, and low," also include pricing for the review activities conducted by the awarded vendor? If not, where should the pricing for the review activities be included on the "Attachment C-Cost Breakdown Offer" sheet provided by the Port?	Submitting vendors should specify their fee structure in the Compensation attachment to the Proposals. You do not need to be limited to the four milestones listed if you would like to break it down further. Please ensure annual costs are clear in your submission that would include (but not be limited to) the four listed milestones on page 3.	Q-001569
96	Is penetration testing part of it?	No	Q-001567
97	Is NIST CSF implemented already and we need to do a surveillance audit?	The framework is implemented. No surveillance audit is necessary.	Q-001567
98	Is this a fresh attempt to implement NIST CSF?	The framework is implemented. The audit is to identify any new gaps over time.	Q-001567
99	What are the objectives and focus areas of these assessments like Risk management, Identity & access Management, threat intelligence and incident response?	Use the NIST CSF as the audit focus.	Q-001567
100	Is third party risk management & audit part of the scope?	No	Q-001567
101	The RFP states that there were annual third-party audits conducted for the last 3 years. Were those audits compl	Yes, it was a contract similar to this RFP. No, we would not provide the results from previous audits.	Q-001566
102	Regarding the Port's Standard Terms and Conditions, would the Port agree to the proposed changes? a. Striking section 27 from the contract terms is recommended as this should not be applicable for the cybersecurity audit. Diagrams related to visualizing audit findings and recommendations could be adequately provided based on the Port's existing documentation (which may include maps and diagrams), but these would be for representative purposes only rather than for use as technical architectural drawings and diagrams as outlined in Section 27. Requiring these diagram standards for reference materials would unnecessarily drive-up project costs. b. Are either time and materials or firm-fixed price proposals acceptable? Different areas of the RFP and Standard Terms and Conditions seem to reflect either approach may be acceptable. Also, some areas of the RFP reflect a desire for just final costs to be provided (e.g. fully weighted number to include any forecasted travel costs), but in other areas it states that reimbursable expenses should be broken out separately. Can this please be clarified to make sure proposals are aligned with the Port's expectations?	Port Currently Reviewing	Q-001566
103	Would you like any technical assessments like vulnerability scans?	No	Q-001560
104	What is the timeframe in which you would like the assessment to be completed? (i.e. 2-3 months	See answerr to question # 93	Q-001560
105	Do we need to consider the $240,000 limit in the case where the two option years are executed or would those be on top of the $240,000 limit for the first 3 years?	$240,000 is the limit for the three year contract and the optional extensions are based on the Port's discretion	Q-001560
106	Would you like a breakdown of lump sum pricing based on estimated hours and hourly rates or would you like it to simply be a lump sum broken out by year?	Lump sum	Q-001560
107	What is the number of employees at the Port?	See question # 1	Q-001558
108	Can we perform our work remotely or is it a requirement for us to do our work on-site?	Yes, the Port would expect virtual work/meetings.	Q-001558
109	What is the number of key IT staff excluding developers at the Port that we would be interviewing?	10-12	Q-001558
110	What is the total number of IT security staff that we would be interviewing?	1	Q-001558
111	How would you assess the Port's security program maturity - low, medium, or high?	Medium to high	Q-001558
112	Is the Port regulated (e.g., PCI, HIPAA, SOX, CMMC, FERPA, etc.)? If yes, please state compliance requirements (e.g., PCI, HIPAA, SOX, etc.).	No	Q-001558

113	• Contract Related: 1. Are we able to add an industry standard clarification to the warranty section to outline the time period under which the services are under warranty and also include a standard warranty disclaimer? These terms are typically addressed in the standard terms of a service provider but are not included in the Port's terms. □ UNLESS OTHERWISE STATED IN A SOW, SERVICE PROVIDER SERVICES ARE WARRANTED FOR THIRTY (30) DAYS FROM THE DATE OF FINAL DELIVERY OF THE SERVICES, DURING WHICH PERIOD SERVICE PROVIDER SHALL PROMPTLY CORRECT ANY DEFECTIVE WORKMANSHIP AT NO ADDITIONAL COST TO CLIENT. SERVICE PROVIDER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AND SPECIFICALLY DISCLAIMS ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT OR ANY WARRANTY ARISING BY USAGE OF TRADE, COURSE OF DEALINGS OR COURSE OF PERFORMANCE. 2. Are we able to add an industry standard limitation of liability to the indemnification section? To the extent allowed under law, this is standard language used for the benefit of both parties to limit damages to a commercially reasonable amount? □ TO THE EXTENT ALLOWED BY LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA, OR USE, INCURRED BY CLIENT OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT, TORT, STATUTORY OR OTHERWISE (ANY LEGAL THEORY), EVEN IF THE OTHER PARTY OR ANY OTHER PERSON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. □ TO THE EXTENT ALLOWED BY LAW AND EXCEPT IN THE EVENT OF A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDICT, BREACH OF CONFIDENTIALITY PROVISION, OR SERVICE PROVIDER'S INDEMNIFICATION OBIGATIONS RELATED TO A THIRD PARTY CLAIM, EACH PARTY'S ENTIRE LIABILITY AND EXCLUSIVE REMEDY FOR DAMAGES FROM ANY CAUSE WHATSOEVER, INCLUDING, BUT NOT LIMITED TO(amount to be included). 3. We (Presidio) have executed the following NASPO agreement and would like to know if this is an option to facilitate the project and govern the T&C's: https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/presidio-networked-solutions-llc/	Port Currently Reviewing	Q-001558
114	Does the Port of Tacoma have a mandatory percentage established on this project for MWBE? If so, could the agency please disclose the percentage?	See answer to question #38.	Q-001557
115	If we are using a subcontractor that is not certified by the Office of Minority and Women's Business Enterprises (OMWBE), will be we disqualified?	No	Q-001557
116	How many points will be reduced on the evaluation criteria if we use a subcontractor that is not certified by the Office of Minority and Women's Business Enterprises (OMWBE)?	None	Q-001557
117	Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?	See Answer to Question #38. This RFP is similar to the incumbent contract with the exception it was a 5-yr contract. Incumbent is eligible to bid on this project.	Q-001556
118	Specify the VLAN details how many are included in the Scope?	This is not a technical audit. We are segmented. Use the NIST CSF.	Q-001556
119	Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?	See information in the RFP	Q-001556
120	How much (%) of the infrastructure is in the cloud?	Not sure why this info is requested. Once again this is not a technical audit.	Q-001556
121	In the IT department/environment, how many employees work?	See question # 1	Q-001556
122	Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?	Both	Q-001556