QUESTIONS & RESPONSES 01

RFQ or RFP / TITLE	**070652 - Information Security Services (Cybersecurity)**
CONTACT	**PROCUREMENT - Attn: 070652**
EMAIL	**procurement@portoftacoma.com**
PHONE NUMBER	**253.383.9436**
PROPOSAL or SOQ DUE DATE	**July 14, 2014 @ 2:00 PM (PST)**
DATE ISSUED	**12-Jun-17**

	PROPOSER QUESTIONS	PORT RESPONSES	RFP Section/Pg
1	My question is: what is the scope of the assets to review? This might affect the bid including 5 team members up to 15 team members.	I am not sure what is being asked here. The scope is clear. Year 1 policies and procedures. Year 2 & 3 testing and an audit in each of the years. Resource it appropriately.	
2	Due to the amount of requested information for Sections 1-3 of the proposal, will the Port consider increasing the maximum pages allowed?	Yes, an additional 5 pages will be allowed.	Section D
3	Under Technical Tasks Year 2 and 3 and the mention of vulnerability assessment and penetration test: o How many external IPs and internal IPs are expected will be in scope for this engagement? o Are there any web applications that will have to be tested? If so: * How many? * What is the size of each web application? o Will the internal penetration test have to be conducted on-site, or will the Port offer remote connection?	*External= as few as 6 and as many as 17 IP addresses. 3 subnets with /24 range Internal= possibly 50 to 100 IP addresses. 7 subnets with /24 range. *Up to 6 websites. Not sure the size of the applications maybe max 200MB. *Onsite testing.	

4	Will the Port of Tacoma consider certifications of a higher (harder) technical degree such as CISSP, GPEN, OPST, GSEC, GWAPT?	Yes.	
5	The IT Systems Disaster Recovery/Continuity Plan is pretty significant project in and of itself. Our process for developing a DR plan involves several components including conducting a business impact analysis (BIA), performing a disaster recovery risk assessment (to identify shortcomings in the existing DR technologies and processes), developing the DR plan itself, then table-top testing the plan. Completing these components could take 4-6 months alone. Is this what the Port had in mind for this task in Year 1?	Yes, this is expected.	
6	For the Technical Tasks, what does the Port envision for the annual information security performance audit? Would it entail assessing how the Port is aligning with NIST's Cybersecurity Framework and DHS/Coast Guard guidelines each year? OR does the Port see the audit as building off of the Cybersecurity Assessment that was initially performed and then gauging how the Port is addressing the deficiencies each year? Please clarify.	We desire to be in some form of compliance with the NIST framework and adhere to the Coast Guard guidelines, The audit will lets us know the areas of deficiencies.	
7	For the annual vulnerability assessment and penetration tests of the Port's networks, please confirm the following: (1) approximate number of external target IP addresses or subnet ranges, (2) approximate number of internal target IP addresses or subnet ranges, and (3) number of wireless networks in scope.	The annual testing is a work in process since this is our first attempt to become compliant. *See question 3 for answer. *See question 3 for answer. *Yes, wireless is in scope.	

8	Does the Port expect the tasks described under "Technical Tasks – Years 2 & 3" to only occur in years 2 and 3 OR will those tasks extend beyond into years 4, 5, etc.?	In the RFP the Technical Tasks years 2 & 3 are to be completed in respected years. Years 4 & 5 are optional if the Port chooses to amend the contract. If the decision to exercise years 4 & 5 the Port will request a quote and will create a PO for the amended services.	
9	We have some team members currently pursuing the cloud-based certifications listed in the Qualifications section. Does not having those certifications preclude a vendor from bidding even though the proposed team has deep knowledge in cloud-based platforms and security?	This would not preclude bidding on the RFP. Having the industry knowledge and best practice is beneficial. However, not having the certs may be a deal breaker if the selection process is close.	
10	What is the vetting process for approval of submitted draft documents and what is the anticipated timeframe for receiving comments after submittal?	As we experience this question, you are asking about the turn around time for draft policy documents. Based on the understanding, the turn around time would be a maximum of 30 days.	
11	Is there an existing standard and or format for policies and procedures that will be required for use? Can you provide details?	The Port does have a standard format for policies and procedures. If selected the template will be provided.	
12	What is your expectation for the amount of the work to be onsite for the policy and procedure development phase? Are there elements of this work that can be completed remotely?	Both on-prem and remote work is required during year one. Initially some on-prem to kick-off each deliverable and gather enough info to work remotely.	
13	For the technical vulnerability and penetration test phase, how many internal nodes (inside the perimeter firewall) and external nodes will be tested? Please consider both subnets to be tested as well as an estimate of live nodes.	See Question 3.	
14	Is social engineering testing considered in-scope or desired for the penetration test portion (includes, email phishing, onsite social, phone social)?	Yes.	

15	Is physical security testing considered in-scope for any phase (e.g. review of clean desk controls, siting protections, data center security, etc? If yes, how many sites to be tested? Please provide addresses – as applicable.	Yes, 7 sites.	
16	For the information security performance audit, how many people or staff will need to be interviewed?	25	