QUESTIONS & RESPONSES 02

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	**June 12, 2017**

	PROPOSER QUESTIONS	PORT RESPONSES	RFP Section
1	With regard to the (5) Policy/Procedure deliverables, do these documents exist in any form currently?	They do not exist.	
2	With regard to the (5) Policy/Procedure deliverables, is there guidance you prefer to use (e.g., NIST)?	Our goal is to align with the NIST framework and Coast Guard guidelines.	
3	For deliverable Number 3, does the Port have a particular set of standards in mind with which you would like the assessment performed?	The Port does not have a standard or practice in mind. We are depending on the expertise of the selected vendor to guide us to best practice.	
4	For deliverable Number 2, does the Port desire both internal and external vulnerability scanning and penetration testing?	Internal, external and wireless is required.	
5	Does the Port have a budget in mind for this project?	No.	
6	Could you please provide the number of servers, applications, and IP addresses that would be in scope for vulnerability scanning and/or penetration testing?	Approximately 120 servers and 40+ apps. External - 3 subnets with /24 ranges. Internal - 7 subnets with /24 ranges.	

7	What is the driver? - The need to provide some form of attestation to clients? - Are you trying to address a regulatory/compliance challenge? - Are you trying to improve maturity of the security program? - Is this an Executive/Board level directive?	Driven by questions 2 & 3.	
8	What type of information is of most importance within the Port?	Commercial contracts, real estate leases, engineering drawing, financial and PII information.	
9	Describe the risk management team and capabilities in place today: - Do they have defined risk roles and responsibilities? (looking for internal audit group, risk analysts, risk managers, a security/risk council or committee, etc.) - When was the last time a risk assessment was conducted? (Note a risk assessment is not the same as a control assessment or security assessment.) - Do you have a risk register with threat scenarios, likelihood/probability, etc.?) - What sorts of policies do you have today and how are they structured?	The port does not have any of these duties or roles in place today.	
10	Do they align, or want to align, to something like NIST 800-53 or ISO 27002? If so, why? NIST 800-53 has a lot of controls and specifics.	If this is in reference to the above questions, yes the need to align with the framework and guidelines stated previously. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.	
11	How many people will be involved in the policy work?	Not sure what is required however, the IT department will be available for most in not all the policy work.	
12	How many target IP's are in scope for assessment?	Less then 200.	
13	How many are internal IP's?	Maybe 150.	

14	How many are external IP's?	Maybe 50.	
15	Is a discovery scan required for this assessment?	No.	
16	Is this for PCI?	No.	
17	Is there a requirement to map to another compliance framework? (IE: HIPAA, ISO, etc…)	No.	
18	Is a retest required?	Possibly.	
19	Will testing be required to be completed afterhours?	Yes.	
20	For Internal Assessment, if we use an internal scanner we will need to know how many hosts to assess the number of scanners, but will also need to know what kind of segmentation the client is using to ensure we have an internal scanner placed in the network to allow us to perform the proper testing. Please describe the network segmentation requiring these additional scanners.	Definitely test the DMZ and production networks. Estimate it at worst case scenario.	
21	Is the Port okay to deploy a virtual scanner for internal IP scanning?	The Port needs to better understand the pros and cons of such a deployment before it can provide a response.	
22	The RFP has been structured in a way that would require work to be performed by services personnel. Our company offers two options for Vulnerability Assessments. One is subscription based and would be on-going throughout the year. The other is a one-time assessment performed by our consulting practice. Is the Port open to receiving information/pricing on both options?	Yes, price both options.	
23	Penetration Testing: How many external target IP's?	See #14.	

24	How many internal target IP's?	See #13.	
25	Can you support VMware for a remote testing appliance related to the internal penetration testing?	We will make this assesment with the selected vendor.	
26	Do you require retesting of High Critical findings?	The assessment should establish this.	
27	Do you require after-hours testing?	Depends, but plan for it.	
28	Is the penetration testing for PCI compliance? - If so how many of the target IP's are PCI related? - Please specify both internal and external requirements.	See #16.	
29	Are you requesting quarterly ASV scans for the external IP's that are in scope for PCI?	No.	
30	Would you like to combine the internal and external penetration testing with an Endpoint Phishing campaign? This combination of testing is referred to as Advanced Penetration Test, and really tests the users security awareness specific to the targeted systems or IP's associated with the goal of obtaining user credentials or gaining direct system access which then is used in conjunction with the internal and external portions of the Advanced Penetration Test. - If this combined test is of interest, please specify how many emails should be included in the campaign specific to the internal and external IP's used in this test.	Yes for the awareness. Only focus on an internal campaign. For the number of emails - what is recommended?	

31	Information Security Assessment – (Annual Performance Audit) - Objective - What are your goals and what are you hoping to achieve with this project.	It entails assessing how the Port is aligning with NIST's Cybersecurity Framework and DHS/Coast Guard guidelines each year.	
32	Drivers - What is driving this initiative now?	See #7.	
33	Project timing - Is there a hard date that you need this work to be completed by?	The RFP clearly outlines the timeline. It is a 3 year contract with the possibility 2 additional years. Year 1 is policies and procedures - years 2 & 3 is testing and audit.	
34	How many sets (single set, multiple sets broken out by business unit) of information security policies do you maintain?	None.	
35	What is the ~size of your information security policies (# of pages) and are they mapped to any particular controls standard (ISO, NIST, Cobit, etc..)	As stated before the Port does not have a policy and yes map it to the framework.	
36	How large is the Port? - # of employees - # of geographic locations - # of business units	300+ employees, 12+ sites, and less than 15 business units.	
37	Is the information security function centralized or do you have multiple business units that are responsible for their own information security. - If multiple, list # of business units and # of individuals responsible for information security within each BU.	Centralized.	
38	Briefly describe your key business processes.	I believe you can get the best feel for the Port of Tacoma and the NW Seaport Alliance at the following websites, www.portoftacoma.com and www.northwestseaportalliance.com.	

39	Briefly describe the systems supporting those processes: - # of servers and type (database, AD, file server, etc..) - # of applications and function (what does the application do?) - # of systems that handle PII data?	12+ SQL servers, 5 DCs, 1 fileserver In the neighborhood of 72 apps. These include app servers, web servers, database servers. 12 different apps in the DMZ and 65 in production. There are 3 systems that may have PII data.	
40	How many people do we need to interview to understand the current state of controls on the systems in-scope and what are their job functions?	6 to 10+.	
41	How many physical sites would be in-scope? In other words, will our consultant have to travel to multiple locations to interview people above?	7 sites (this includes Pier 69 (Port of Seattle Admin Bldg.))	
42	Describe what [y]our standard deliverables look like	We don't have a particular standard for a deliverable. It is task dependable.	