QUESTIONS & RESPONSES #2

RFP / TITLE	**070076 IT Cybersecurity Assessment and Plan**
CONTACT	**Michael Keim, CPPB, Sr. Contract Adminstrator**
EMAIL	**procurement@portoftacoma.com**
PHONE NUMBER	**253-428-8608**
SUBMITTAL DUE DATE	**Monday, February 23, 2015 @ 4:00 P. M.**
Q&A ISSUE DATE	**Thursday, February 12, 2015**

PROPOSER QUESTIONS	PORT RESPONSES
While the Port mentions the inclusion of areas B.a to B.e under Scope of Services, is it also expected that the Consultant review and assess other aspects of the Port's cyber security posture such as system patching, data backup, incident response, disaster recovery, segregation of duties, physical security of the data center, etc.?	Yes
Is vulnerability assessment scanning and penetration testing expected to be performed on the Port's network perimeter, internal systems, and wireless networks?	Yes
If vulnerability assessment scanning and penetration testing is expected to be performed, please indicate the number of external targets, internal targets, and wireless networks.	The Port understands "targets" to mean IP addresses and as such, the following information is provided: internally we have private class A, B, and C. Externally we have class B and C.
How many servers does the Port manage? Please indicate physical vs. virtual.	See previously posted Question - Answer 1, line 11; http://portoftacoma.com/contracts/procurement/070076/it-cybersecurity-assessment-and-plan
How many end users are there?	230
How many IT staff are there?	15

What is the number of workstations supported?	258
What is (are) the server operating system(s) utilized at the Port?	MS Windows 2008 & 2012
What are the major applications in use at the Port?	The Port is a Microsoft shop for both servers and workstations. This means the Port utilizes email, unified communications, SQL, IIS, CRM, and GP. There are a number of exception we also use IBM Maximo and GIS.
Is social engineering expected to be part of this assessment? (Please indicate what type of testing is desired: spear phishing, phone-based, physical penetration testing, etc.)	Email phishing & phone-based.
Do you want any web applications assessed?	Yes
How many nodes are in scope?	1000+
Will the assessment be done from an internal or external perspective or both?	Both
Does the Port of Tacoma currently have asset management/asset tracking capability? If yes, please describe the format (e.g., spreadsheet, database, software application, etc.)	We are a typical business utilizing the Microsoft product stack for both the servers and workstations.
Will the Port of Tacoma authorize the utilization of the successful offeror's IT asset discovery/asset inventory application to facilitate cyber security analytics?	Possibly, it is open for discussion.
Will port of Tacoma require—and authorize—net security penetration testing or similar network scanning service(s)?	Possibly, it is open for discussion.
What is the desired level of complexity for assessment? Are red-team probes and attacks or simulations desired?	This project has a fixed cost, not to exceed $100K. It is in the Port's interest to achive the best valued assessment for our money.
What is the scale of their system? Can you provide a system diagram to outline the scope?	This information will be provided to the selected Consultant.
Who is the current vendor who has done the IT Cybersecurity Assessment and Plan from the past?	There is no current vendor nor has this work been done in the past.
Who manages the current IT Department?	This question has no bearing on the Scope of Work or other details contained in this RFP.
Could you please tell me what the current costs are for this solicitation and how can I obtain a copy of the contract?	Please read the RFP - Background Section regarding current costs for this solicitation. There is no current nor previous contract for this work.
Please confirm contract period of performance end date—9/19/2016 or 9/19/2015.	2016

Port Text: All policies shall be issued by a company having an A. M. Best rating of A:VI or better. Exception: Professional Liability insurance is maintained through ABS Boiler & Marine Insurance Company ("ABS BMIC"), a Vermont insurer. As a captive insurer owned by our ultimate parent company, parent company (and our company) is not rated by A.M. Best or any other rating agency. Therefore, we need to take an exception to this effect.	No waiver or exception to the Port's insurance requirements will be granted.
Port text: Each insurance policy shall be endorsed to state that coverage shall not be suspended, voided, canceled or reduced in coverage or limits except after 45 days prior written notice has been given to the Port. Exception: Our underwriters will not endorse our policies in such a fashion; a decision over which we have no control. Remedy: Consultant will provide the Port with any notice of cancellations or material changes in the policies in accordance with policy terms.	No waiver or exception to the Port's insurance requirements will be granted.
In regards to the IT Cybersecurity Assessment and Plan RFP you posted, we were wondering if you had reverse engineering malware and/or exploits in mind as part of this RFP?	Please read Q&A #1, Line 15 found on the Port's website: http://portoftacoma.com/contracts/procurement/070076/it-cybersecurity-assessment-and-plan
How many and what type of firewalls are in place?	Five, Palo Alto
Is administration of systems centralized or de-centralized?	Centralized
How many external (Internet facing) IP addresses does Port of Tacoma have/own that should be considered as in-scope for external testing?	We have six external facing subnet and yes include it in the scope.
How many websites are running from the Port of Tacoma's infrastructure?	None, a third party vendor hosts the website.
Please list the number of different operating systems and web servers (i.e. IIS, Apache, etc…) that are running.	Windows 2008 & 2012 OS. Primarily an IIS shop with on exception with one IBM application using Apache.
Please describe the Internet facing systems/applications run by Port of Tacoma that are hosted on in-house systems.	Currently, only I-Pro. This will not be available to check as it owned by a third party, is proprietary and is locked-down.
Please list any Internet facing systems that are conducting some form of e-commerce.	None
Please describe each form of remote access provided to staff, IT, and/or vendors	Microsoft TMG and UAG is used for remote access.

Are there any hosted applications (not on your infrastructure) that should be considered in-scope for this assessment?	None
How many Wireless Access Points are in use?	14
Is just a review of configurations or active penetration test on the wireless network desired? If the latter, how many locations will need to be tested for the wireless penetration test?	The latter and the minimum of three locations.
How many separate wireless networks are there?	2
How many data centers are to be tested?	1
How many internal IP addresses are active? Or in general, how many subnets are in use?	See question 13.
Do you have any SCADA or industrial control systems that are used and would be in scope?	None
Are there any special security clearances needed or citizenship requirements to perform the work?	No particular clearances necessary. U.S. citizenship is strongly encouraged.
Are there any specific instructions: 1.) restrictions 2.) limitations on what percentage of the work can be performed remotely or on premise.	Restrictions and limitations will be determined once a vendor is selected.
How many servers, switches, OS's, Virtualization, applications and security devices are in scope? Traditional IP, Ddos. UC Unified Communications, Communications network based, T-dos,	140 servers, 67 switches, 5 firewalls, Microsoft OS, Hyper-V, Lync for the UC.
What are the product vendors of the network infrastructure: switches, routers, firewalls, Unified Threat Management platforms, Intrusion Detection, VPN, RDP, Web Application Firewalls, and or other security devices, or APT tools. This will help to determine the best tools for the assessment. Is Encryption in use, type, full disc, database, file, email, are HSM's in use, has PKI or RMS, CAC cards, IAM in use?	Cisco = switches, routers, and wireless. Firewalls = Palo Alto. We are a Microsoft shop = TMG, SQL Email and the like. No PKI or RMS
What types of Applications Are in Scope? Are there any bespoken mobile or Web applications or custom applications, databases?	Email, IIS, SQL, and Lyn. No custome apps.
Is physical security assessment included in the SOW, and or social engineering of staff or other 3rd party vendors that may have access?	Yes
Are there any other framework(s) or compliance guidelines that the security assessment should be measured against – NIST//SSI? Are there any other Compliance Measurements for consideration: NERC-CIP, CJIS, (PCI, SOX, Federal, State, Local privacy or security laws, etc) *The SOW only recognizes the NIST framework as outlined in the specific Executive Order.	This is the expertise the Port is wanting the vendor to guide us in. What else should be considered?

Is anything outsourced to a 3rd party or to a cloud provider, do we need to notify any other parties or obtain permissions to conduct any assessments?	We are just starting to work with Microsoft Office 365.
External Vulnerability//Internal//Wireless//How many IP Ranges are in scope?	See question 49
How many physical points of presence will need to be visited for the wireless portion of the assessment?	3 to 5 is sufficient.
Is detection of rogue wireless access points in scope for the project?	Since there are 14 WAPs it is expected.
How many firewalls and types of firewalls are in-scope for the configuration validation?	See question 53. Only four are in scope.
Is there an expectation that this project will include a review of firewall rules?	Yes
How many operating systems and database platforms are in-scope for the configuration validation?	See questions 18-19
How many network segments and IP addresses are in the overall environment?	See question 49
Are there any web applications in-scope, and is there an expectation that web application scanning will be performed?	Web scanning to be performed.
Are any third parties, hosted, or outsourced components in-scope?	None
Are there any SCADA (supervisory control and data acquisition) or similar types of systems or networks in-scope?	see question 50
Will reference questionnaires be subject to public disclosure? If so, will the description of services and reference name and contact information be subject to public disclosure?	Please review the Section - Public Disclosure contained in Attachment A - Instructions for Proposing of the RFP.
What is the size of the internal infrastructure? (Subnet size, number of hosts, etc.)	See questions 49 and 53
What is the size of the external infrastructure? (Subnet size, number of hosts, etc.)	6 subnets, 13 hosts
Number of routers	2
Number of firewalls	5
Number of wireless networks	2
Number of CCTV systems	1
Number and type of servers	See RFP Question - Answer 1, question 11; http://portoftacoma.com/contracts/procurement/070076/it-cybersecurity-assessment-and-plan
You mention web servers but no specific web applications or websites for assessment. How many web apps or sites are you looking at for the assessment?	Less then 10.

For the Web Application Assessment, can a brief description of the size and functionality be provided? (What is the approximate total number of pages and approximate number of input/dynamic pages (such as web forms where users input data) each external web application under scope supports?	Don't have a number of total pages. There are 10 web servers internally for such apps as SharePoint, HR, CRM, and GIS. Externally there are only a few web apps HR and IBM Maximo.
For the Wireless Assessment: How many locations and an approximate number of access points or size of the facility?	No greater than six locations. All within a two mile radius of the admin bldg.
For Social Engineering: Is this limited to email phishing or are there specific Social engineering use cases that the Port of Tacoma would like to have performed?	Email phishing is included in the scope.
Will the assessment be conducted during normal business hours?	Yes
Is there any limitation to the hours in which scanning / penetration testing can be performed?	No restrictions.
Are you using NIST framework today?	DHS and the Coast Guard require it. Tthe Port would like to know where it is at physically and get a road map as a result of the assessment to assist with understanding this beast.
What framework are you looking to have the policies and procedures evaluated against? 800-53, ISO-27001, NIST Cybersecurity Framework, other?	Initially NIST. Followed by recommendations as a result of the assessment.