QUESTIONS & RESPONSES #01

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
Please let us know what is the number of end users in scope for this assessment.	Approximately 300 users
Are you looking for a gap assessment or a formal assessment with certification?	Gap Assessment
How many locations are in-scope?	3-5 sites
How many disaster recovery locations are in-scope?	2
How many IT personnel will be in-scope?	20
How many security personnel will be in-scope?	1
How many systems (i.e., servers, workstation) are in-scope of the assessment?	See information in the RFP
How many employee users can access systems within the scope?	See answer to question #1.
How many systems are accessible from the internet?	None
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.
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
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.
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.
When was the last agencywide risk assessment performed?	2005
Did the risk assessment include IT and Cybersecurity risks?	No
Do these IT risk assessments include or consider outsourced functions, third parties, and business partners?	No
What does the Port currently consider to be its most serious cybersecurity risks?	The human elemnet
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

Has the Port formally documented data classification and prioritization of systems?	Yes
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
Does the Port maintain established roles and responsibilities over cybersecurity?	Yes
Does the Port have a security incident response plan?	Yes
Does the Port perform Tabletop exercises periodically?	Yes
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
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