Vendor Cybersecurity Risk Self-Assessment Tool

Revised Apr 2024

1. The vendor shall use this self assessment tool to evaluate it's cybersecurity posture and expectations for safeguarding the Port of Tacoma/NWSA against cyber-attacks emanating from the vendor's network, products, services, and/or applications.

2. The "**Vendor Cybersecurity Assessment Controls**" column lists a series of questions the vendor shall answer in the "**Vendor Self Assessment Score (Degree of Compliance)**" column, adding comments and/or caveats to clarify the response in the "**Vendor Clarification Comments**", if necessary.

3. The vendor shall enter an appropriate numerical score (1, 2, or 3) in the "**Vendor Self Assessment Score (Degree of Compliance)**" column to reflect its self assessed degree of compliance for each control. For example, the vendor shall enter a "1" in response to the question "Does every user have an individualized login, meaning "No" generic users?" if every employee and/or contingent staff member working for the vendor has an individualized Login ID and Password, or a "2" if some employees, contingent staff, or support vendors share a Login ID and/or Password.

4. The vendor can enter remarks that clarify the numerical score (1, 2, or 3) assigned to a question in the "**Vendor Clarification Comments**" column if the vendor believes that clarification of the score is necessary or would be beneficial to the vendor; comments are optional. For example, the vendor could enter a comment such as "Employees, contingent workers, and all of our vendors are assigned unique Login IDs and passwords, which are coupled with cell phone-based multifactor authentication to access our network, products, services, and applications."

5. The vendor should contact the Port Contracts and Purchasing team member that sent them the questionnaire if there are questions about any of the questions in this questionnaire. Ideally, the vendor will "bundle" all of the questions about completing the questionnaire into a single clarification request back to the Port to help speed and improve the efficiency of the process.

6. After completing the questionnaire, the vendor shall:

   a. Save a copy of this tool, replacing the word TEMPLATE-RFP with your company name; and
   b. Include a copy of the saved response file back with their proposal submitted to the RFP.

7. **The vendor shall be prepared to participate in a follow up call with the Port's IT team and provide non-proprietary supporting evidence to verify its responses and/or comments in the questionnaire, if requested.**

The blue text in the table below is for illustrative purposes and should be replaced with vendor-specific responses.

				Vendor Risk Assessment	
Vendor Name	**Self Assessment Year**	**Self-Assessment Category**	**Vendor Cybersecurity Assessment Controls**	**Vendor Self Assessment Score (Degree of Compliance)** **1 - Yes** **2 - Yes, with Caveats** **3 - No**	**Vendor Clarification Comments (Comments required for an Score of 2 or 3)**
		GENERAL	Does your firm conduct background checks on all employees and contingent workers before hiring or contracting with them?		
			Does your firm comply with a cybersecurity framework?		
		PASSWORD AND IDENTITY MANAGEMENT:	Does every user have an individualized login, meaning "No" generic users?		
			Are network credentials hidden from each vendor/user?		
		LEAST PRIVILEGED ACCESS CONTROLS:	Does your firm implement a least privilege policy for all users?		

			Is your firm able to limit employee, contingent worker, and/or vendor access to:		
			Only necessary network segment(s)?		
			Only the specific server/system(s)?		
			Only specific application port(s)?		
			Only specific periods of time needed for access?		
			Does your firm have an easy provisioning and de-provisioning process for user access privileges?		
			Are privileged access permissions documented for each user?		
			Does your firm conduct regular reviews of user privileges to reassess access requirements?		
		MONITORING AND AUDIT CONTROLS:	Is a network admin notified of each new employee, contingent worker, or vendor session?		
			Do network managers have the ability to approve or deny individual user sessions?		
			Are admins able to review the details of every user session?		
			Are granular logs kept of vendor activities down to keystroke level?		
			Are video logs captured to view sessions?		
			Does your firm keep logs for an extended period of time (minimally 6 months)?		
			Does your firm maintain an inventory of all active 3rd party users?		
		Training, Response, and Management Plans	Does your firm provide cybersecurity training for your employees and contingent staff? NOTE: Please describe the training, including how frequently it is conducted, in the Comments section.		
			Does your firm have a cybersecurity incident response plan?		
			Does your firm have a disaster recovery plan?		
			Does your firm have a vendor cybersecurity management plan?		
			Vendor Cybersecurity Self-Assessment Score	**0**	